D-Link DES-3010G/3018 3026

ユーザマニュアル

Layer2 10/100M Managed Switch

目次

本書の使い方

DES-3010G/DES-3018/DES-3026 ユーザマニュアルは以下のセクションに分かれており、システムの設置と操作方法を例題とともに説明しています。

セクション 1 はじめに – 本スイッチの特長について説明しています。

セクション 2 設置方法 – スイッチの基本的な設置方法とともに導入に方法について説明しています。さらに前面パネル、背面パネル、側面パネル、および LED 表示について説明しています。

セクション 3 スイッチの接続 – ご使用のネットワークに本スイッチを接続する方法について説明しています。

セクション 4 スイッチマネージメントの概要 – パスワードプロテクション、SNMP 設定、IP アドレス割り当て、スイッチへのデバイスの接続など基本的な本スイッチの管理機能について紹介しています。

セクション 5 Web ブラウザを使用したスイッチの設定 – 本スイッチに実装された Web ベーススイッチマネージメント機能への接続、および使用方法について説明しています。

セクション 6 スイッチの管理 – スイッチ情報へのアクセス方法、スイッチのユーティリティの使用方法、ネットワーク設定方法など以下に示すような本スイッチの基本機能を設定する方法について詳しく説明しています。IP アドレス割り当て、ポート設定、ユーザアカウント、ポートミラーリング、システムログ設定、SNTP、TFTP、Ping Test、SNMP、シングル IP マネージメント、フォワーディング&フィルタリング。

セクション 7 レイヤ 2 機能 – VLAN、トランキング、IGMP Snooping、およびスパニングツリーなど本スイッチのレイヤ 2 機能について説明しています。

セクション 8 セキュリティ – トラフィックコントロール、ポートセキュリティ、802.1X、トラストホスト、およびトラフィックセグメンテーションなど本スイッチのセキュリティ機能について説明しています。

セクション 9 CoS– 本スイッチの Quality of Service 機能について詳しく説明しています。

セクション 10 モニタリング – 本スイッチの機能およびパケットをグラフィック画面でモニターする機能について説明しています。

付録 A 製品の仕様 - DES-3010G、DES-3018、DES-3026 およびオプションの主な仕様について説明しています。

付録 B ケーブルとコネクタ - RJ-45 プラグ/コネクタ、ストレート/クロスケーブル、および標準的のピンアサインについて説明しています。

付録 C ケーブル長 – ケーブルタイプとケーブル長(最大)に関する情報を記載しています。

用語解説 – 本マニュアル内で使用する項目の定義について説明しています。

本マニュアルの対象者

DES-3010G/DES-3018/DES-3026 ユーザマニュアルは 本スイッチの設定および管理について記載しています。本マニュアルはネットワーク管理の概念と専門用語を使用しておりネットワーク管理者向けに記載しています。

表記について

表記	説明
[ ]	コマンドラインインタフェースでオプションを示します。 例：[copy filename] はオプションで copy の後にファイル名を入力します。 ([ ] は入力しません。)
Bold font	・ボタン、ツールバーアイコン、またはメニュー項目を強調するために使用します。 例：**File** メニューから **Cancel** を選択します。 ・画面上のシステムメッセージやプロンプトを表すこともあります。また、ファイル名、プログラム名、およびコマンドを表示します。 例： **You have mail**.
`Boldface Typewriter Font`	入力プロンプトでマニュアルに記載とおりに入力する必要のあるコマンドやレスポンスを示します。
Initial capital letter	画面名を表します。キーボード上のキーの名前は先頭が大文字で示します。 例：Enter をクリックします。
Italics	画面名またはフィールドを表します。また、単語や文字列に置き換えられる変数やパラメータを表します。 例：「*filename* を入力します。」は本当のファイル名を *Italics* で示した単語の替わりに入力することを意味します。
Menu Name > Menu Option	**Menu Name > Menu Option** はメニュー構造を示します。**Device > Port > Port Properties** は、Device メニューの下の Port メニューの Port Properties メニューオプションを表しています。

参照、注意、および警告

確認 はデバイスのよりよい使用方法に関する重要な情報を表します。

注意 は潜在的なハードウェアの損傷やデータの損失を知らせ、その問題を回避する方法を示します。

警告 は所有物の破壊、使用者の傷害または死亡が想定される内容について示しています。

安全上のご注意（必ずお守りください）

本製品を安全にお使いいただくために、以下の項目をよくお読みになり必ずお守りください。

警告　この表示を無視し、まちがった使いかたをすると、火災や感電などにより人身事故になるおそれがあります。

注意　この表示を無視し、まちがった使いかたをすると、傷害または物損損害が発生するおそれがあります。

してはいけない「**禁止**」内容です。

必ず実行していただく「**指示**」の内容です。

警告

分解禁止

分解・改造をしない

機器が故障したり、異物が混入すると、やけどや火災の原因となります。

禁止

落としたり、重いものを乗せたり、強いショックを与えたり、圧力をかけたりしない

故障の原因につながります。

禁止

発煙、焦げ臭い匂いの発生などの異常状態のまま使用しない

感電、火災の原因になります。使用を止めて、ケーブル/コード類を抜いて、煙が出なくなってから販売店に修理をご依頼してください。

ぬれ手禁止

ぬれた手でさわらない

感電のおそれがあります。

水ぬれ禁止

水をかけたり、ぬらしたりしない

内部に水が入ると、火災、感電、または故障のおそれがあります。

禁止

油煙、湯気、湿気、ほこりの多い場所、振動の激しいところでは使わない

火災、感電、または故障のおそれがあります。

禁止

内部に金属物や燃えやすいものを入れない

火災、感電、または故障のおそれがあります。

禁止

表示以外の電圧で使用しない

火災、感電、または故障のおそれがあります。

禁止

たこ足配線禁止

たこ足配線などで定格を超えると火災、感電、または故障の原因となります。

禁止

設置、移動のときは電源プラグを抜く

火災、感電、または故障のおそれがあります。

禁止

雷鳴が聞こえたら、ケーブル/コード類にはさわらない

感電のおそれがあります。

禁止

ケーブル/コード類や端子を破損させない

無理なねじり、引っ張り、加工、重いものの下敷きなどは、ケーブル/コードや端子の破損の原因となり、火災、感電、または故障につながります。

禁止

正しい電源ケーブル、コンセントを使用する

火災、感電、または故障の原因となります。

禁止

乳幼児の手の届く場所では使わない

やけど、ケガ、または感電の原因になります。

次のような場所では保管、使用をしない

禁止

・直射日光のあたる場所

・高温になる場所

・動作環境範囲外

禁止

光源をのぞかない

光ファイバケーブルの断面、コネクタ、および製品のコネクタをのぞきますと強力な光源により目を損傷するおそれがあります。

注意

静電気注意

コネクタやプラグの金属端子に触れたり、帯電したものを近づけますと故障の原因となります。

コードを持って抜かない

コードを無理に曲げたり、引っ張りますと、コードや機器の破損の原因となります。

振動が発生する場所では使用しない

接触不良や動作不良の原因となります。

禁止

付属品の使用は取扱説明書にしたがう

付属品は取扱説明書にしたがい、他の製品には使用しないでください。

機器の破損の原因になります。

セクション 1

はじめに

本マニュアルは DES-3010G/DES-3018/DES-3026 スイッチグループの設置、設定、およびメンテナンスを説明しています。これらのスイッチの基本的なハードウェア構成は似ており、設定方法、操作性はほぼ共通です。また、本マニュアル内の記載事項の多くが共通です。

Web 画面は、シリーズの中の一製品を例にとって説明していますが、ポート数を除き設定方法は同じです。このドキュメントではスイッチの例題、設定、および説明に DES-3018 を主に使用しています。

スイッチ設定

DES-3010G/DES-3018/DES-3026 はハイパフォーマンスの 8/16/24 ポートファーストイーサネットスイッチです。Auto MDI-X/MDI 機能を搭載した 10/100Mbps の UTP ポートによって構成されています。また、多くのマルチメディアを要求し、ボトルネックを作らないでネットワーク上でのイメージングアプリケーションを有効にする光接続を小規模でかつ下位に接続するネットワークに分割するためのスイッチです。これらのポートはさらに PC、プリンタ、サーバ、ハブ、ルータ、スイッチ、および他のネットワークデバイスを接続するために使用することができ、full-duplex モードで最大 200Mbps スループットをサポートします。

DES-3018 / DES-3026 モデルの拡張スロットと DES-3010G のギガビットポートはサーバまたはバックボーンへのアップリンクを提供します。実装されたコンソールインタフェースはプライオリティキュー、VLAN、およびポートトランキンググループのためのスイッチの設定やポートのモニター、ポート速度の設定のために使用されます。

特長

- IEEE 802.3z 準拠
- IEEE 802.3x Flow Control 準拠(フルデュプレックス)
- IEEE 802.3u 準拠
- IEEE 802.3ab 準拠
- IEEE 802.1p Priority Queues

- IEEE 802.3ad Link Aggregation Control Protocol
- IEEE 802.1X Port-based および MAC-based Access Control
- IEEE 802.1Q VLAN
- IEEE 802.1D Spanning Tree および IEEE 802.1W Rapid Spanning Tree
- シングル IP マネージメント
- SNTP(Simple Network Time Protocol)
- システムとポートユーティリザーション
- システムログ
- 速度の適応とプロトコル変換のためのノンブロッキングストア&フォワード
- ポートごとのイーグレス/イングレスレート制御
- ポートベースの有効/無効
- MAC アドレス: 最大 8K
- 柔軟なロードディストリビューションとフェイルオーバ機能を持つポートトランキング
- IGMP Snooping
- SNMP
- SMTP
- CPU アクセスコントロールリスト
- ポートミラーリング
- MIB: RFC1213 MIB II、RFC1493 Bridge、RFC1757 RMON、RFC1643 Ether-like MIB、RFC2233 Interface MIB、RFC2358 Ether-like MIB、IF MIB、Private MIB、RFC2674 for 802.1p、IEEE 802.1X MIB、
- スイッチ管理のための RS-232C コンソールポート
- Link/Act、ポートスピードなどポートステータスのための LED 表示

イーサネットテクノロジー

ファーストイーサネットテクノロジー

LAN の重要性の増加とアプリケーションの複雑さの増加により高性能ネットワークの必要性が高まっています。多くの高速 LAN テクノロジーがさらに広い帯域を提供し、クライアント/サーバのレスポンスタイムを改善するために提案されています。それらの中でファーストイーサネット(100BASE-TX)は 10BASE-T テクノロジーからスムーズに発展しています。

100Mbps ファーストイーサネットは IEEE 802.3 LAN 委員会が指定する標準規格です。CSMA/CD (Carrier Sense Multiple Access with Collision Detection) イーサネットプロトコルで制御を行いながら 100Mbps でデータを送受信する能力を持つ 10Mbps イーサネット標準規格の拡張機能です。

ギガビットイーサネットテクノロジー

ギガビットイーサネットは同じパケット構造と形式を利用し、CSMA/CD プロトコルサポート、フルデュプレックス、フローコントロール、および管理オブジェクトを利用する IEEE 802.3 イーサネットの拡張機能で、理論スループットは 100Mbps ファーストイーサネットの 10 倍、10Mbps イーサネットの 100 倍です。ギガビットイーサネットは、すべての 10Mbps および 100Mbps イーサネットと互換性があるため、既存のハードウェア、ソフトウェア、および習熟した個人への会社の投資を無駄にせずに簡単にアップグレードできます。

ギガビットイーサネットが提供する速度の高速化と帯域幅の増加は、コンピュータとそのバスがさらに高速になり、より多くのユーザが多量のトラフィックを生成するアプリケーションを使用するために頻繁に発生するネットワークのボトルネックへの対処に不可欠です。バックボーンおよびサーバなどのキーコンポーネントをギガビットイーサネットにアップグレードすることで、サブネットワーク間のトラフィックを著しくスピードアップするのはもちろんネットワークレスポンスタイムを大きく改善することができます。

ギガビットイーサネットはビデオカンファレンス、複雑な映像処理、および同じデータが集中するアプリケーションをサポートする高速光ファイバ接続を有効にします。同様にデータ転送がファーストイーサネットの 10 倍であるため、ギガビットイーサネットを装備したサーバは同じ時間で 10 倍の処理を行うことができます。

さらにギガビットイーサネットが提供する非常に大きな帯域は今日、明日に瞬く間に改善されていくスイッチングおよびルーティングインターネットワーキングテクノロジーを利用するもっともコスト効果の高い方法です。

スイッチングテクノロジー

イーサネットテクノロジーの限界を押しのける別のキーとなる開発はスイッチングテクノロジーのフィールドにあります。スイッチは接続しているイーサネットまたはファーストイーサネット LAN セグメント内に転送するイーサネットプロトコルの MAC アドレスレベルでイーサネットパケットをブリッジします。

スイッチングはローカルエリアネットワーク上のユーザに有効なネットワーク総容量を増大させるコスト効果の高い方法です。スイッチは容量を増加させ、ローカルエリアネットワークが異なるセグメントに分離することを可能にすることでネットワークローディングを減少させます。そのためネットワーク転送容量をお互いに競うことなく、各セグメント上のロードを減少させることができるのです。

スイッチは個別のセグメント間でもっとも最速を選択してブリッジします。スイッチは1つのセグメントから別のセグメント(1つのポーから別のポート)に送信する必要のあるトラフィックをその他のセグメント(ポート)を妨害しないで自動的に転送します。これは同じネットワークの接続およびアダプタカードを維持しながらネットワーク総容量を増加させます。

ファーストイーサネットまたはギガビットイーサネットにとってスイッチは、"two-repeater limit"を超えてつながれているハブの問題を取り除く効果的な方法です。例えばご使用のファーストイーサネットネットワークを 100BASE-TX ネットワークの限界であり 205m を超えて拡張することを可能にするなどスイッチは異なるネットワークをコリジョンドメインに分割するために使用します。スイッチは従来の 10Mbps イーサネットと 100Mbps ファーストイーサネットの両方をサポートしており既存の 10Mbps ネットワークと新しい 100Mbps ネットワーク間のブリッジもします。

スイッチング LAN テクノロジーはネットワークブリッジの従来型を著しく改良しており、より高い潜在能力によって特徴つけられています。ルータはまた、ローカルエリアネットワークをセグメント化するために使用されていますが、ルータのコストや要求される設定、メンテナンスをスイッチと比較すると実際の導入が難しい場合があります。本スイッチは雑多なローカルエリアネットワークの集中による問題を理想的に解決します。

前面パネルと LED 表示

スイッチの前面パネルは Power、Console、Link/Act、Speed の LED、8/16/24 ファーーストイーサネットポート、2つの拡張ポート(DES-3018/3026 のみ)、1000BASE-T ポート(DES-3010G のみ)、および SFP ギガビットイーサネットとポート(DES-3010G のみ)を搭載しています。さらに RS-232C ポートを搭載しています。

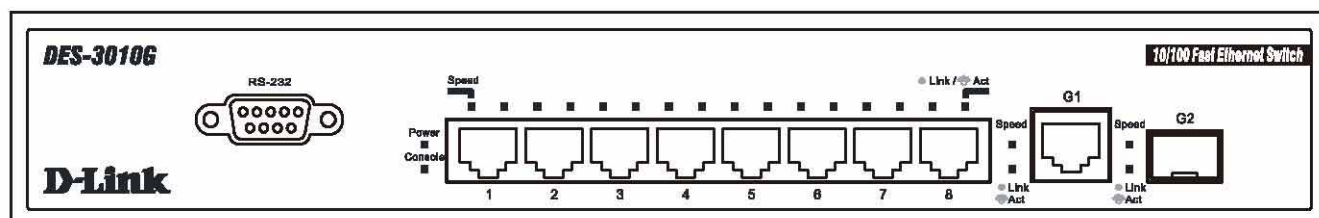



図1- 1. DES-3010G の前面パネル

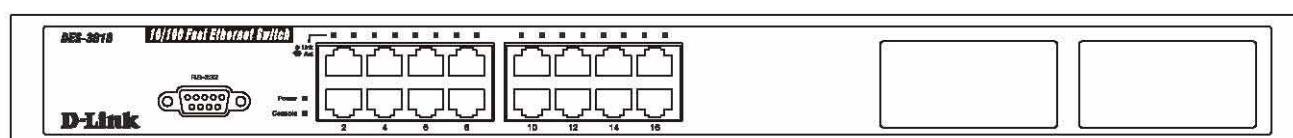



図1- 2. DES-3018の前面パネル

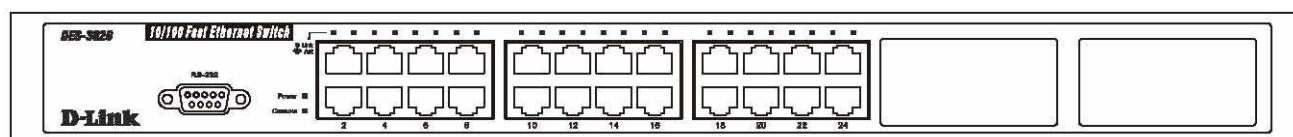



図1- 3. DES-3026の前面パネル

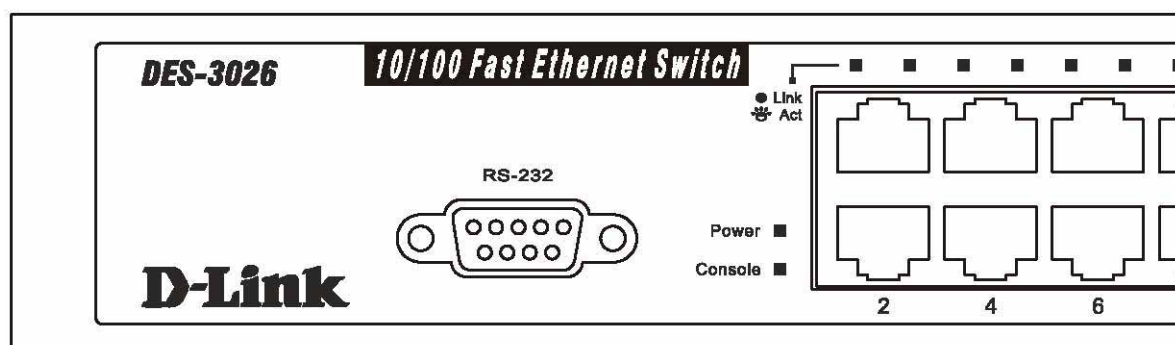



図1- 4. DES-3026の LED 表示

LED 表示はスイッチとネットワークのステータスを表示します。

LED	色	状態	説明
Power	緑	点灯	電源が供給され正常に動作しています。
	ー	消灯	電源オフなどで電源を供給されない場合は消灯します。
Console	緑	点滅	Power-On Self Test (POST)中点滅し、終了すると消灯します。
	ー	点灯	コンソールポートのリンクが確立しています。
Link/Act	緑	点灯	DES-3010G: リンクが確立しています。 DES-3018/3026: 100Mbpsでリンクが確立しています。
	緑	点滅	DES-3010G: データを送受信しています。 DES-3018/3026: 100Mbpsでデータを送受信しています。
	橙	点灯	DES-3018/3026: 10Mbpsでリンクが確立しています。
	橙	点滅	DES-3018/3026: 10Mbpsでデータを送受信しています。
	ー	消灯	リンクが確立していません。
Speed **(DES-3010G)**	緑	点灯	100Mbpsでリンクが確立しています。
		消灯	10Mbpsでリンクが確立しているか、またはリンクが確立していません。
Link/Act(G1) **(DES-3010G)**	緑	点灯	リンクが確立しています。
		点滅	データを送受信しています。
	ー	消灯	リンクが確立していません。
Speed(G1) **(DES-3010G)**	緑	点灯	1000Mbpsでリンクが確立しています。
		消灯	10Mbps/100Mbpsでリンクが確立しているか、またはリンクが確立していません。
Link/Act(G2) **(DES-3010G)**	緑	点灯	1000Mbpsでリンクが確立しています。
		点滅	1000Mbpsでデータを送受信しています。
	ー	消灯	リンクが確立していません。
Speed(G2) **(DES-3010G)**	緑	点灯	1000Mbpsでリンクが確立しています。
		消灯	リンクが確立していません。

背面パネル

スイッチの背面パネルには電源コネクタがあります。

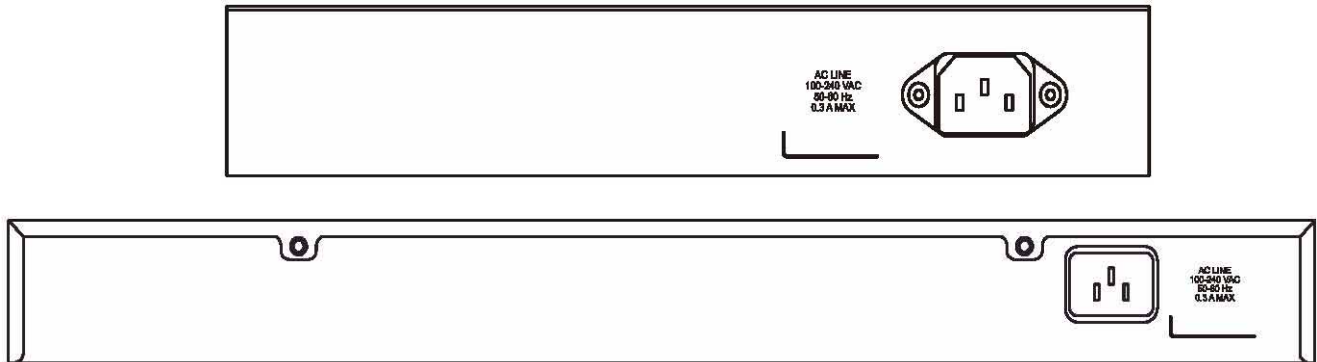



図1- 5. DES-3010G(上)と DES-3018/DES-3026(下)の背面パネル

側面パネル

スイッチの両側面には熱を放出する通気口があります。これらをふさがないようにご注意ください。スイッチの適切な通気のためには、少なくとも 16cm 以上のスペースを確保してください。最適な熱放出、空気の循環をしないとシステム障害や部品の激しい損傷を引き起こす場合がありますのでご注意ください。

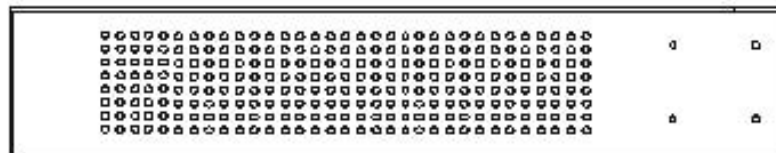



図1- 6. 側面パネル

セクション 2

設置方法

パッケージの内容の確認

設置のためのガイドライン

ゴム足の取り付け(19インチラックに取り付けない場合)

19インチラックへの取り付け

電源をオンにする

オプションモジュール

パッケージ内容の確認

ご購入いただいたスイッチの梱包箱を開け、同梱物を注意して取り出してください。以下のものが同梱されています。

1. 本体 x 1
2. 電源ケーブル x 1
3. ラックマウントキット 1 式(ブラケット 2 枚、ネジ)
4. ゴム足(貼り付けタイプ) x 4
5. RS-232C コンソールケーブル
6. CD-ROM x 2
7. 製品保証書

万一、不足しているもの損傷を受けているものがありましたら、交換のために弊社ホームページにてユーザ登録を行い、サポート窓口までご連絡ください。

設置のためのガイドライン

本スイッチを安全に設置いただくために以下のガイドラインにしたがってください。

- 最低 3kg の重量を支えられる場所で設置を行ってください。本スイッチ上に重たいものを置かないでください。
- 本スイッチから 1.82m 以内の電源コンセントを使用してください。
- 電源ケーブルを確認し、電源ポートに危険がないことを目で確認してください。
- 本スイッチの周辺で熱の放出と充分な換気ができることを確認してください。換気のためには少なくとも 製品の前後 10cm は空間を空けてください。
- 本スイッチの動作温度と動作湿度に適応した涼しく湿度の低い場所にスイッチを設置してください。
- モーターのような強力な磁力を発生する機械、振動、ほこり、および直射日光に当たる場所を避けて本スイッチを設置してください。

直接机の上などに設置する場合は、本スイッチの底面にゴム足を取り付けて設置してください。ゴム足がクッションになり設置面を傷つけることを防ぎます。

ゴム足の取り付け(19 インチラックに設置しない場合)

デスクトップまたは棚に設置する場合、はじめに本スイッチ付属のゴム足を取り付けてください。スイッチ裏面の 4 隅に貼り付けます。充分な通気のために他のものは離して設置してください。

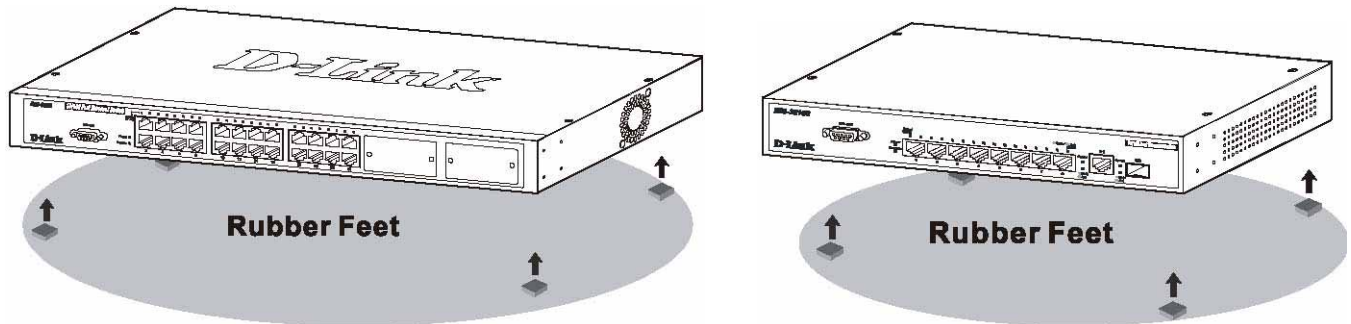



図 2- 1. ゴム足の取り付け(デスクトップまたは棚に設置する場合)

19 インチラックへの取り付け

以下の手順に従って本スイッチを標準の 19 インチラックに設置します。

ブラケットの取り付け

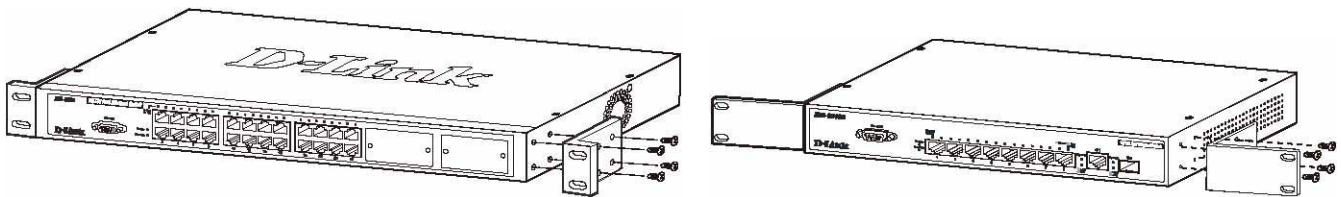



図 2- 2. ブラケットを取り付ける

ラックマウントキットに付属のネジを使用して、本スイッチにブラケットを取り付けます。完全にブラケットが固定されていることを確認し、本スイッチを以下のとおり標準の 19 インチラックに固定します。

19 インチラックにスイッチを取り付ける

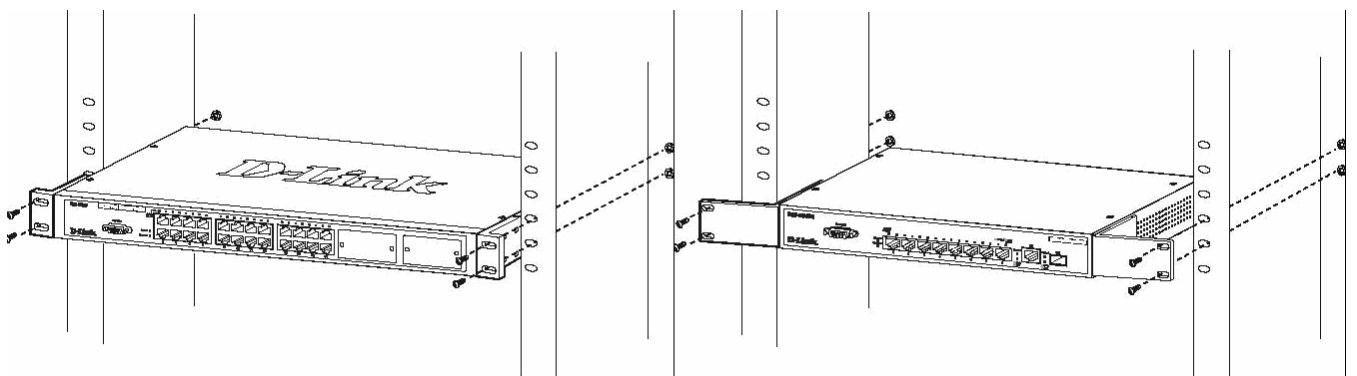



図 2- 3. スイッチを19インチラックに設置する

電源をオンにする

1. 電源ケーブルを本スイッチの電源コネクタに接続します。電源ケーブルのプラグを電源コンセントに接続します。
2. 本スイッチに電源が供給されると Power LED が点灯します。システムのリセット中、LED は点滅します。

オプションモジュール

DES-3018 と DES-3026 の前面パネル右にオプションの拡張モジュール用の空きスロットがあります。これらのオプションモジュールは本スイッチシリーズ用に特別に設計されており、サーバまたはコアスイッチへのアップリンクのために使用します。このスロットはシングルポートアップリンクモジュール(別売)を装着します。以下にオプションモジュールについて説明します。

DEM-301T

・ シングルポート 1000BASE-T ギガビットイーサネットアップリンクモジュール

・ IEEE 802.3、IEEE 802.3u、IEEE 802.3ab 準拠

・ Speed、Link、Act の LED 搭載

・ 10/100/1000M オートネゴシエーション(フルデュプレックスの場合)、バックプレッシャー(ハーフデュプレックスの場合)、IEEE 802.3x フローコントロール(フルデュプレックスの場合)サポート

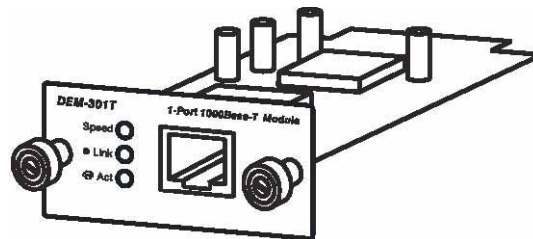



図 2- 4. DEM-301T オプションモジュール

DEM-301G

・ シングルポート SFP ギガビットアップリンクモジュール

・ IEEE 802.3z 準拠

・ Link/Act の LED 搭載

・ オートネゴシエーション(フルデュプレックスの場合)、IEEE 802.3x フローコントロール(フルデュプレックスの場合)サポート

・ DEM-310GT、DEM-311GT、DEM-314GT、DEM-315GT サポート

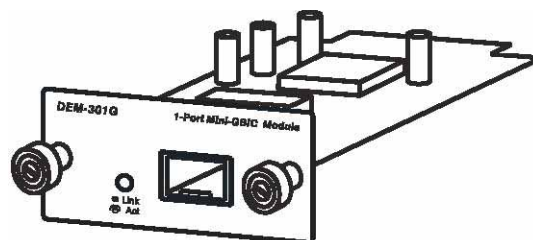



図 2- 5. DEM-301G オプションモジュール

以下の手順に従ってモジュールを装着します。

警告: オプションモジュールを取り付ける前に、本スイッチからすべての電源ケーブルまたはケーブル類が取り外されていることを確認してください。取り外さないで行うと感電、故障の原因になります。

スイッチ前面右側にオプションモジュール用のスロットがあります(図 2-7 と図 2-8)。スロットにはスロットカバーが取り付けられています。モジュールを取り付ける場合は、スロットカバーのネジをゆるめてはずします。

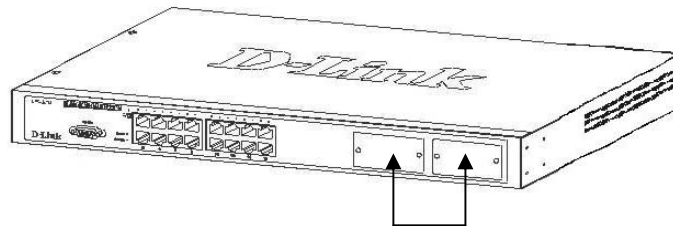



図 2- 8. DES-3018前面パネルの拡張モジュールスロット

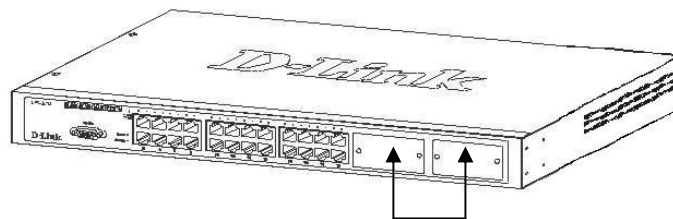



図 2- 9. DES-3026前面パネルの拡張モジュールスロット

以下の図のように本スイッチのスロット内の奥に到達するまでモジュールをスライドさせます。注意しながらモジュールをゆっくりと固定します。次に本スイッチのネジ穴とモジュールを合わせて2つのネジで固定します。

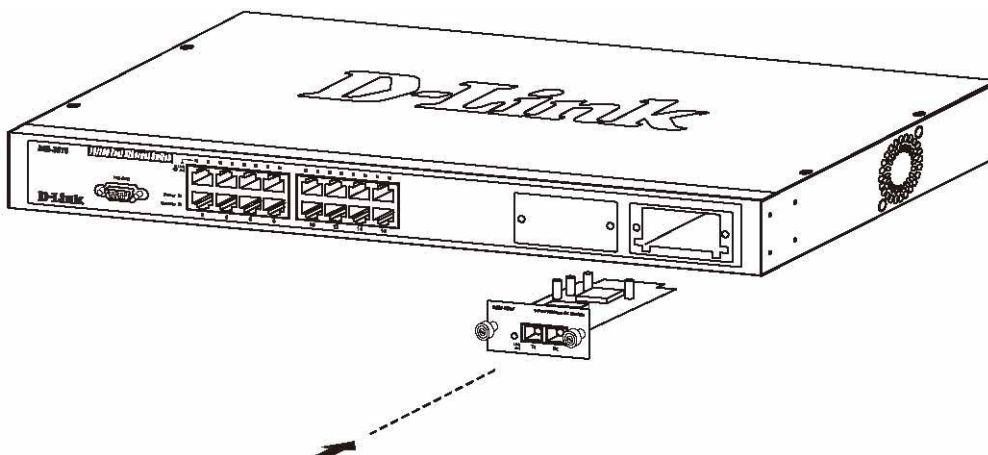



図 2- 10. オプションモジュールの取り付け

DES-3018 / DES-3026 のアップグレードが終了しました。

セクション 3

スイッチの接続

エンドノードと接続する

スイッチ同士を接続する

バックボーンまたはサーバに接続する

確認: すべてのイーサネットポートは Auto MDI/MDI-X をサポートしています。

エンドノードと接続する

エンドノードとは 10/100/1000 Mbps RJ-45 ネットワークカード(NIC)およびルータなどを指します。

本スイッチの 1000BASE-T ポートとエンドノードを UTP/STP ケーブルを使用して接続します。

エンドノードはスイッチの 10BASE-T/100BASE-TX ポートに接続します。

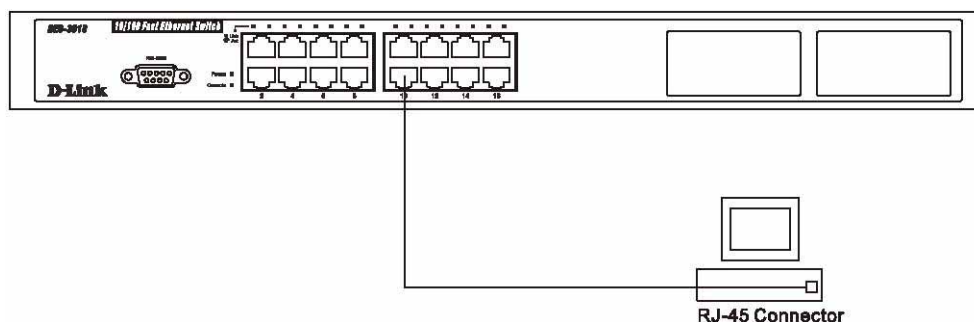



図 3- 1. エンドノードとスイッチの接続

エンドノードと正しくリンクが確立すると本スイッチの各ポートの Link/Act LED は緑色または橙色に点灯します。データの送受信中は点滅します。

スイッチ同士を接続する

使用するケーブルによって以下のように接続します。

- カテゴリ 3 以上の UTP/STP ケーブル: 10BASE-T ハブまたはスイッチと接続します。
- カテゴリ 5 以上の UTP/STP ケーブル: 100BASE-TX ハブまたはスイッチと接続します。
- エンハンスドカテゴリ 5 以上の UTP/STP ケーブル:1000BASE-T スイッチと接続します。
- 光ファイバケーブル: 本スイッチの SFP ポートと光ファイバアップリンクを搭載するスイッチと接続します。

ケーブル仕様については付録 B を参照してください。

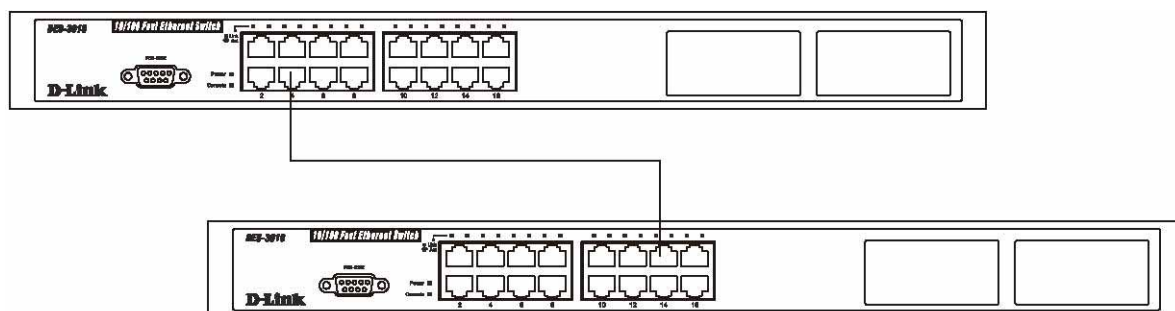



図 3- 2. ストレートまたはクロスケーブルでスイッチ間を接続する

バックボーンまたはサーバに接続する

限られた空間で多くのイーサネット接続を要求するオフィスやビルのネットワークバックボーンとして DES-3010G/3018/3026 を使用することができます。高速ラインが ISP と接続すると DES-3010G/3018/3026 は PC、プリンタ、ハブ、ルータ、または別のスイッチを含むさまざまなエンドノードを接続します。そのトポロジー設定は無限ですが、ボトルネックにならないように DES-3010G/3018/3026 からの接続が ISP へのアップリンクと同じか遅いということに注意してください。

RJ-45 ポートはフルまたはハーフデュプレックスモードで 100Mbps もしくは 10Mbps の速度で動作します。100BASE-FX ポートはフルデュプレックスモードでだけ 100Mbps で動作可能です。RJ-45 ギガビットポートはフルデュプレックスモードでだけ 1000Mbps で動作可能です。SFP ギガビットポートはフルデュプレックスモードでだけ 1000Mbps で動作可能です。

ギガビットイーサネットポートの接続にはポートのタイプに応じて光ファイバケーブルまたはエンハンスドカテゴリ 5 ケーブルを使用します。正しく接続すると Link LED が点灯します。

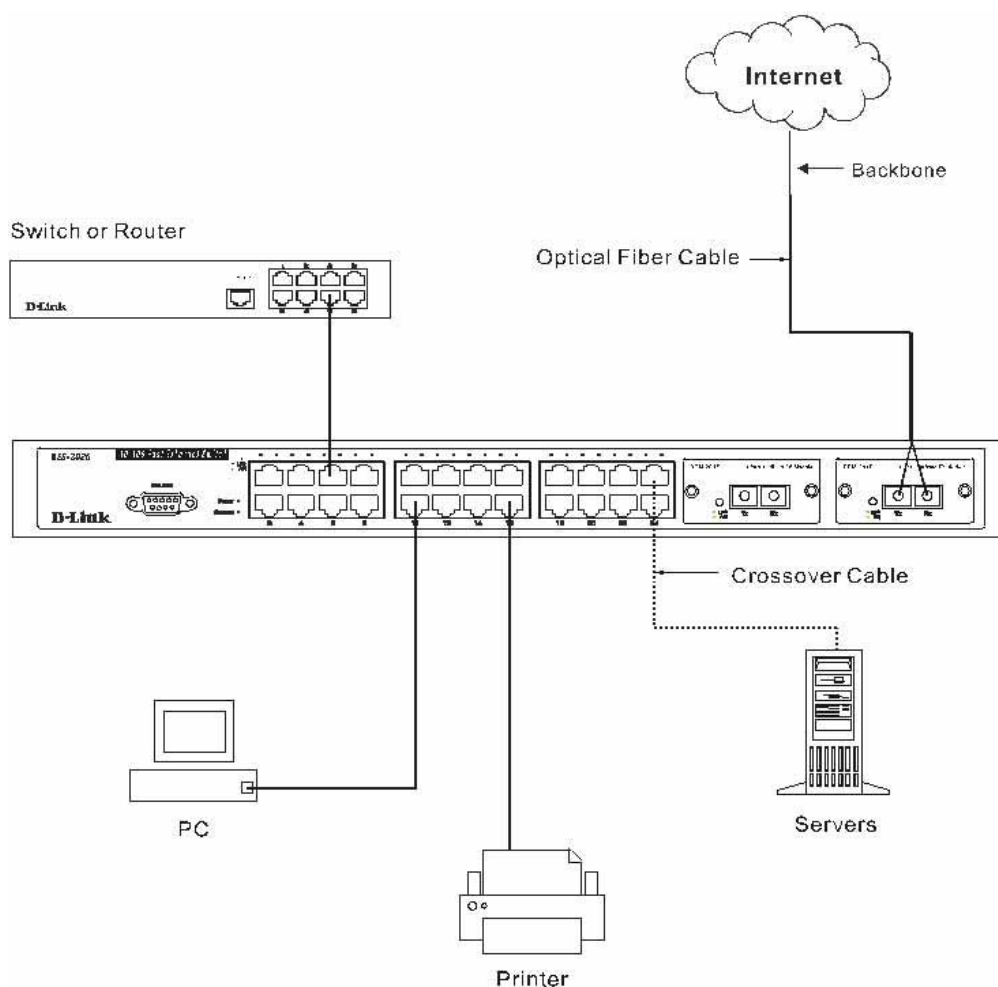



Figure 3- 3. サーバ、PC、スイッチスタックへのアップリンク接続

セクション 4

スイッチマネージメントの概要

マネージメントオプション

本システムはコンソールポートを経由したアウトオブバンド、または Telnet を使用したインバンドにより管理されます。Web ブラウザによっても管理することができます。

Web ベースマネージメントインタフェース

本スイッチの設置完了後、Netscape Navigator (version 6.2 以上) または Microsoft® Internet Explorer (version 5.0 以上) によって本スイッチの設定、LED のモニター、および統計情報をグラフィカルに表示することができます。

SNMP ベースマネージメント

SNMP サポートするコンソールプログラムでスイッチの管理をすることができます。本スイッチは SNMP v1.0、v2.0、および v3.0 をサポートしています。SNMP エージェントは、受信した SNMP メッセージをデコードし、データベースに保持している MIB オブジェクトを持つリクエストに返信します。SNMP エージェントは MIB オブジェクトを更新し、統計情報およびカウンタ情報を生成します。

シリアルポート経由の CLI(Command Line Console Interface)

コンピュータまたは端末をコンソールポート経由で本スイッチに接続できます。CLI(コマンドラインインタフェース)により本スイッチの管理機能のすべてを使用できます。

コンソールポートに接続する(RS-232C DCE)

スイッチのモニタリングと設定のために RS-232C シリアルポート(D-Sub9 ピン)を搭載しています。

コンソールポートを使用するためには以下をご用意ください。

- ターミナルソフトを操作するシリアルポート搭載の端末またはコンピュータ
- D-Sub-9 ピン メスコネクタを持つヌルモデムケーブル、または RS-232C クロスケーブル

端末をコンソールポートに接続する:

1. RS-232C ケーブルの一方を直接本スイッチのコンソールポートに接続し、付属のネジで抜けないように固定します。
2. ケーブルのもう一方を端末またはターミナルソフトが動作するコンピュータのシリアルコネクタに接続します。以下の手順でターミナルソフトを設定します。
3. **接続の設定**画面の**接続方法**でシリアルポート (**COM** ポート)を選択します。
4. 選択したポートの**プロパティ**画面で **9600 ビット/秒**にデータ速度を設定します。
5. **データビット**は **8**、**ストップビット**は **1**、**パリティ**は**なし**に設定します。
6. **フロー制御**は**なし**に設定します。
7. **エミュレーションモード**を **VT100** に設定します。
8. **ファンクションキー、方向キー、Ctrl キーの使い方**で**ターミナルキー**を選択します。**ターミナルキー**(Windows キーではない) の選択を確認します。

確認: Microsoft® Windows® 2000 ハイパーターミナルを使用する場合、Windows 2000 Service Pack 2 以降がインストールされていることをご確認ください。Windows 2000 Service Pack 2 以降でないとハイパーターミナルの VT100 端末で矢印キーは使用できません。Windows 2000 service pack に関する情報はマイクロソフト社のホームページでご確認ください。

9. 端末設定の完了後、本スイッチに電源ケーブルを接続し、電源プラグをコンセントに接続します。ブートシーケンスが端末上に表示されます。
10. ブートシーケンスが完了すると、コンソールのログイン画面が表示されます。
11. 購入後はじめてログインする場合は、ユーザ名(UserName)とパスワード(PassWord)プロンプトで Enter キーを押します。本スイッチにはユーザ名(UserName)とパスワード(PassWord)の初期値はありません。はじめに管理者によるユーザ名(UserName)とパスワード(PassWord)の作成が必要です。すでにユーザアカウントを作成している場合は、ログインし、続けて本スイッチの設定をします。
12. コマンドを入力して設定を行います。コマンドの多くは管理者レベルのアクセス権が必要です。次のセクションでユーザアカウントの設定について説明します。CLI のすべてのコマンドリストおよび追加情報については CD-ROM に収録された **Command Line Interface Reference Manual** を参照してください。
13. 管理プログラムを終了する場合は、**logout** コマンド使用するか、ターミナルソフトを終了します。

端末上で接続に問題が発生した場合は、ターミナルソフトの設定で**エミュレーション**が **VT-100** となっていることを確認してください。**エミュレーション**はハイパーターミナル画面の**ファイル**メニューから**プロパティ**をクリックし、**設定**タブにて設定します。何も表示されない場合はスイッチの電源を切り再起動してください。

コンソールに接続すると、以下のようにコンソール画面が表示されます。ここで管理機能を実行できます。ユーザ名とパスワードの入力プロンプトが表示されます。初期接続ではユーザ名とパスワードは設定されていないため、2 回 **Enter** を押して CLI に接続します。

```
            DES-3018 Fast Ethernet Switch Command Line Interface

                        Firmware: Build 3.00.032
        Copyright(C) 2004-2007  D-Link Corporation. All rights reserved.
UserName:
```

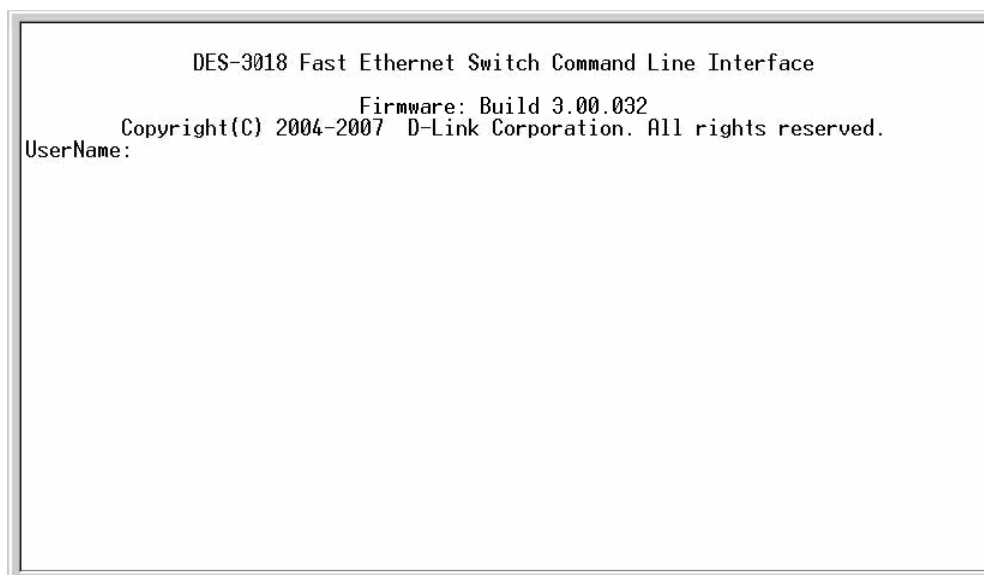



図 4- 1. 最初に接続時の初期画面

スイッチにはじめて接続する

本スイッチは本スイッチへのアクセス権限のないユーザのアクセスや設定変更を防ぐセキュリティ機能をサポートしています。このセクションではスイッチにログインする方法を説明します。

確認: パスワードは大文字小文字を区別します。

例 「S」と「s」は別の文字として判断します。

本スイッチにはじめて接続すると次のログイン画面が表示されます。

確認: Ctrl+R でコンソール画面のリフレッシュをします。

```
              DES-3018 Fast Ethernet Switch Command Line Interface

                              Firmware: Build 3.00.032
        Copyright(C) 2004-2007  D-Link Corporation. All rights reserved.
UserName:
```

図 4- 2. はじめてスイッチに接続したときの初期画面

はじめての接続のときには UserName または PassWord は登録されていません。**UserName** と **PassWord** フィールドには入力せず、Enter を押します。すでに設定されている場合は、UserName と PassWord の両方を入力します。

以下の画面のように **DGS-3018:4#**というコマンドプロンプトが表示されます。:

```
              DES-3018 Fast Ethernet Switch Command Line Interface

                              Firmware: Build 3.00.032
        Copyright(C) 2004-2007  D-Link Corporation. All rights reserved.
UserName:
PassWord:
DES-3018:4#
```

図 4- 3. コマンドプロンプト

確認: はじめにログインしたユーザが自動的に管理者権限を取得します。少なくとも一つは管理者レベルのユーザカウントを作成する必要があります。

パスワード設定

本スイッチシリーズは初期値として UserName と PassWord を持っていません。はじめにユーザアカウントの作成を行います。定義済みの管理者レベルの UserName でログインすることでスイッチ管理ソフトウェアに接続できます。

はじめてログインした際に本スイッチに対する不正アクセスを防ぐために UserName に対して必ず新しいパスワードを定義してください。このパスワードは忘れないように記録しておいてください。

管理者レベルのアカウントを作成する手順は以下のとおりです。

1. ログインプロンプトで「create account admin <*user name*>」を入力します。
2. パスワード入力プロンプトが表示されます。管理者アカウントに使用する<*password*>を入力します。
3. 入力後、確認のために再度同じ入力プロンプトが表示されます。同じパスワードを入力します。
4. 新しい管理者の作成が成功すると画面に"Success" と表示されます。

確認: PassWord(パスワード)は大文字小文字を区別します。UserName と PassWord は 15 文字以内の半角英数字を指定してください。

以下は新しい管理者レベルユーザの UserName に newmanager を指定する手順の例です。

```
DES-3018:4#create account admin newmanager
Command: create account admin newmanager

Enter a case-sensitive new password:********
Enter the new password again for confirmation:********

Success


DES-3018:4#
```

注意: CLI 設定コマンドは動作中の設定だけが変更され、本スイッチを再起動すると消去されます。**save** コマンドを使用してすべての設定をフラッシュメモリ(NV-RAM)に格納する必要があります。

SNMP 設定

SNMP（簡易ネットワーク管理プロトコル）は OSI 参照モデルの第7層（アプリケーション層）のプロトコルで、ネットワークデバイスの管理やモニタリングを行います。ネットワーク管理デバイスは、SNMP を利用してゲートウェイ、ルータ、そしてその他のネットワークデバイスの設定状態の確認や変更ができます。SNMP を利用してシステムの設定を行い、適切なオペレーション、パフォーマンスのモニタリング、デバイスまたはネットワーク全体に潜在する障害検知を行います。

SNMP をサポートする管理デバイスは、スイッチ上で動作する SNMP エージェントと呼ばれるソフトウェアを備えています。SNMP エージェントは管理オブジェクトの変数定義を保持し、デバイスの管理を行います。管理オブジェクトは MIB として定義され、デバイスの SNMP エージェントにより管理される情報表示の基準を（管理側のデバイスに）伝えます。SNMP は MIB（情報管理ベース）仕様およびネットワークを介して（管理デバイスに）送信される際のプロトコルのフォーマットを定義しています。

本スイッチシリーズは、SNMP のバージョン 1（SNMP v1）、2c（SNMP v2c）、および 3（SNMP v3）を実装しています。この3種類の SNMP により管理側とネットワークデバイス間のセキュリティレベルを調整します。SNMP v1 と v2c は、ユーザ認証において SNMP コミュニティ名をパスワードのように利用します。リモートユーザ SNMP（エージェント）と（管理側の）デバイスは同一のコミュニティ名に所属している必要があります。SNMP では認証されないメッセージは破棄されます。

SNMP の v1 または v2c（のデバイスや管理ソフト）の初期状態で設定されているコミュニティ名は次のとおりです。

- **public** -（ネットワークデバイス SNMP 管理ソフトに）MIB オブジェクトの読み出し権限が許可されているコミュニティ名です。
- **private** – MIB オブジェクトの読み出しと書き込みの権限を与えられているコミュニティ名です。

SNMP v3 には（旧バージョンより）2 種類の拡張された認証プロセスがあります。SNMP マネージャとしてのユーザリストとユーザ属性の機密性維持することと、リスト上のユーザごとに SNMP マネージャとしてのアクセス制限を設定できることです。

リスト上のユーザに対してアクセス制限を定義します。（対応する）SNMP のバージョンは SNMP マネージャのグループごとに設定されます。よって、読み取り権限の定義、または SNMP v1 を使用したトラップ受信を可能にした SNMP マネージャグループと SNMP v3 を利用した読み取りと書き込みの権限を付与したグループをグループごとに作成できます。SNMP v3 を利用して個々のユーザや SNMP の管理グループは特定の SNMP 管理機能の実行や制限を設定できます。SNMP 管理機能は特定の MIB に関連した MIB オブジェクトである OID を利用して許可／拒否を定義します。

スイッチの SNMP v.3 設定方法に関する詳細についてはセクション 6 を参照してください。

トラップ(Trap)

トラップとはネットワーク上で発生したイベントをマネージャに通知するメッセージのことです。トラップメッセージ（イベント通知）にはネットワークデバイスのリブート（再起動）などの重大なイベントやネットワーク状態変化があります。ネットワークデバイスでイベントが発生した場合、（エージェントは）あらかじめ指定したマネージャに対してトラップメッセージを送信します。通知できるイベントは認証エラー、ネットワーク状態変化、およびブロードキャスト/マルチキャストストームなどです。

MIB

ネットワークデバイスに実装された MIB(情報管理ベース)には、デバイスの管理情報を格納しています。ネットワークデバイスは標準的なネットワークデバイス管理情報として MIB-Ⅱをサポートしています。MIB オブジェクト（と呼ばれるデバイスの情報）の値を SNMP 管理ソフトにより取得します。本スイッチは標準的な MIB-Ⅱに加えて拡張 MIB をサポートします。OID と呼ばれる MIB オブジェクトの識別子を定義することで拡張 MIB の情報を取得します。MIB の値は読み取り専用のものと読み取りと書き込みが可能なものがあります。

IP アドレスの割り当て

各スイッチには IP アドレスを割り当てる必要があります。IP アドレスは SNMP ネットワークマネージャまたは他の TCP/IP アプリケーション(例：BOOTP、TFTP)と通信をするために使用されるため、スイッチごとに必要です。本スイッチの IP アドレスの初期値は未設定の 10.90.90.90 です。はじめにご使用のネットワークアドレス構成にあわせて本スイッチの IP アドレスの初期値を変更してください。

本スイッチは MAC アドレスが割り当てられています。以下のように CLI で **show switch** と入力することで参照することができます。

```
Command: show switch

Device Type         : DES-3018 Ethernet Switch
Module 1 Type       : None
Module 2 Type       : None
MAC Address         : 00-11-95-EB-83-32
IP Address          : 10.53.13.33 (Manual)
VLAN Name           : default
Subnet Mask         : 255.0.0.0
Default Gateway     : 0.0.0.0
Boot PROM Version   : Build 1.01.005
Firmware Version    : Build 3.00.032
Hardware Version    : 0A1
System Name         :
System Location     :
System Contact      :
Spanning Tree       : Disabled
IGMP Snooping       : Disabled
802.1X              : Disabled
TELNET              : Enabled(TCP  23)
WEB                 : Enabled(TCP  80)
RMON                : Disabled

DES-3018:4#
```

図 4- 4. "show switch" コマンドによって表示された情報

本スイッチの MAC アドレスは Web ベースの管理インタフェースの **Switch Information** メニューに表示されます。

本スイッチの IP アドレスは Web ブラウザの使用前に設定する必要があります。本スイッチの IP アドレスは BOOTP または DHCP プロトコルを使用して自動的に設定することもできます。この場合はスイッチに割り当てられたアドレスは既知のものとなります。

IP アドレスはコンソールから CLI を使用して設定します。

コマンドラインプロンプトで以下のとおりコマンドを入力します。:

config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy

xxx.xxx.xxx.xxx は IP アドレスを示し、**System** と名づけた IP インタフェースに割り当てられます。**yyy.yyy.yyy.yyy** は対応するサブネットマスクを示しています。

または **config ipif System ipaddress xxx.xxx.xxx.xxx/z** と入力することもできます。**xxx.xxx.xxx.xxx** は IP インタフェースに割り当てらた IP アドレスを示し、**z** は CIDR 表記で対応するサブネット数を表します。

本スイッチ上の **System** という名前の IP インタフェースに IP アドレスとサブネットマスクを割り当てます。設定が完了すると管理ステーションから本スイッチの Telnet または Web ベースの管理エージェントに接続できるようになります。

```
DES-3018 Fast Ethernet Switch Command Line Interface

Firmware: Build 3.00.032
Copyright(C) 2004-2007  D-Link Corporation. All rights reserved.
UserName:
PassWord:
DES-3018:4#config ipif System ipaddress 10.53.13.33/255.0.0.0
Command: config ipif System ipaddress 10.53.13.33/8

Success

DES-3018:4#
```

図 4- 5.　スイッチに IP アドレスを割り当てる

上記の例では、255.0.0.0 のサブネットマスクを持つ IP アドレス 10.53.13.33 を本スイッチに割り当てています。コマンドが正しく実行されると **Success** が表示されます。これで本スイッチは Telnet と CLI、または Web ブラウザ経由で本スイッチの設定および管理を行うことができます。

スイッチにデバイスを接続する

スイッチに IP アドレスを割り当てた後、スイッチにデバイスを接続することができます。

SFP トランシーバポートにデバイスを接続する手順は以下のとおりです。:

- 接続する環境に対応する SFP トランシーバタイプを選択します。
- SFP トランシーバスロットに SFP トランシーバ(別売)を装着します。
- ネットワーク環境に合わせ、SFP トランシーバのコネクタにデバイスを接続します。

注意: SFP トランシーバがリンクすると、コンボポートの 10BASE-T/100BASE-TX/1000BASE-T ポートは無効になります。

セクション 5

Webブラウザを使用したスイッチの設定

はじめに

本スイッチシリーズの機能は組み込まれている Web ベース(HTML)インタフェース経由で管理、設定およびモニターができます。標準のブラウザを使用してネットワーク上のリモートステーションから本スイッチを管理します。ブラウザは HTTP プロトコルを使用し、スイッチと通信します。

本スイッチの設定および確認は、Webブラウザ、コンソール接続、またはTelnet接続で行います。ここではWebブラウザを利用した方法について説明します。

Web ブラウザにログインする

はじめにコンピュータでブラウザを起動し、本スイッチに定義したIPアドレスを入力します。ブラウザのアドレスバーに以下のようにURLを入力します。例: http://123.123.123.123（123.123.123.123 はスイッチのIPアドレス。）

確認: 初期状態ではIPアドレス「10.90.90.90」、サブネットマスク「255.0.0.0」が設定されています。端末側のIPインタフェースを本スイッチにあわせるか、本スイッチを端末側のIPインタフェースにあわせてください。

以下の画面で **Login** をクリックします。:

図 5- 1. ログインボタン

以下のユーザ認証画面が表示されます。

図 5- 2. ログイン画面

ユーザー名フィールドと**パスワード**フィールドを空白のまま **OK** ボタンをクリックします。Web ベースユーザインタフェースに接続します。Web ブラウザによって使用可能な機能を以下で説明します

Web ベースユーザインタフェース

Web ブラウザでスイッチの設定、管理の画面にアクセスし、パフォーマンス状況やシステムステータスをグラフィック表示で参照できます。

ユーザインタフェースのフレーム

以下のとおりユーザインタフェースは3つのフレームで構成されています。

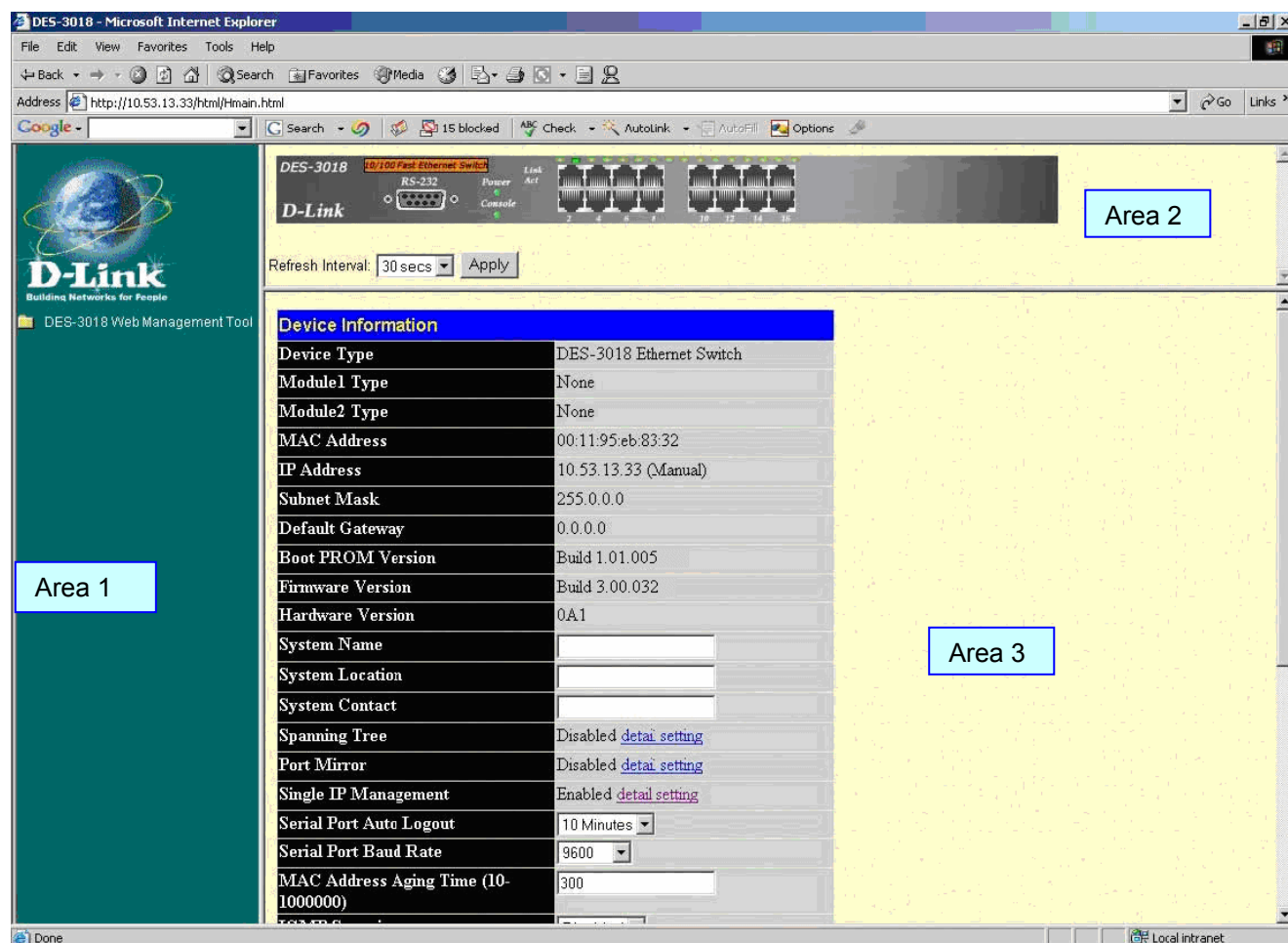



図 5- 3. メイン Web ブラウザ画面

エリア	機能
Area 1	メニューまたは画面表示のために選択します。フォルダを開き、ハイパーリンクメニューボタンとサブフォルダをクリックし、メニューを表示します。D-LinkロゴをクリックするとD-Linkのホームページに接続します。
Area 2	本スイッチの前面パネルを画像で表示します。このフレームは指定モードによりポートの通信状態、デュプレックスモード、またはフローコントロール制御状況を表示します。また、スイッチのポートや拡張モジュールを表示します。 ポート設定を含む管理機能はここで設定できます。
Area 3	選択したスイッチ情報と設定データのエントリを表示します。

注意: スイッチ設定を変更した場合、以下で説明する Web ブラウザの Save Change 画面またはコマンドラインインタフェース(CLI)の save コマンドにて保存する必要があります。

Web ページ

Web ブラウザで本スイッチに接続し、ログイン画面でユーザ名とパスワードを入力し本スイッチの管理モードにアクセスします。

以下はWebブラウザで使用可能なメインフォルダ、メインフォルダに続くメニュー、およびサブディレクトリの一覧です。:

Administration – IP Address, Port Configuration, User Accounts, Port Mirroring, System Log Settings, SNTP Settings, MAC Notification Settings, TFTP Services, Ping Test, SNMP Manager, Ping Test, SNMP Manager, IP-MAC Binding, Single IP Setting, Forwarding & Filtering および SMTP Service

L2 Features – Static VLAN Entry, Trunking, IGMP Snooping および Spanning Tree

CoS – Port Bandwidth, 802.1p Default Priority, 802.1p User Priority, CoS Scheduling Mechanism, CoS Output Scheduling, Priority Settings, TOS Priority Settings, DSCP Priority Settings, Port Mapping Priority Settings および MAC Priority

CPU Interface Filtering – CPU Interface Filtering State および CPU Interface Filtering Table

Security – Traffic Control, Port Security, Port Lock Entries, 802.1X, Trusted Host および Traffic Segmentation

Monitoring – CPU Utilization, Port Utilization, Packets, Packet Errors, Packet Size, MAC Address, Switch Log, Log Settings, IGMP Snooping Group, Browse Router Port, Browse ARP Table, Session Table および Port Access Control

Reset, **Reboot System**, **Save Changes** および **Logout**

確認: 安全のためにネットワークに接続する前にユーザ名とパスワードを必ず設定してください。

セクション 6

スイッチの設定

デバイス情報

Device Information 画面では本スイッチの **MAC** アドレス(工場出荷時に設定され、変更不可)、**Boot PROM**、**Firmware Version** および **Hardware Version** が表示されます。この情報は PROM のトラックを保持するためやファームウェアの更新のために必要であり、本スイッチを別のネットワークデバイスへエントリする場合に使用します。また、**System Name**、**System Location**、および **System Contact** の設定が行えます。Spanning Tree、MAC Notification、ポートミラーリング、シングル IP マネージメントの機能には Detail settings リンクがあり、これをクリックすることで各設定ページにアクセスすることができます。これによりネットワーク管理者は直ちに参照可能であるためスイッチ機能に関係する問題に対応できます。

図 6- 1. デバイス情報画面

IP アドレス

ネットワーク接続前に IP アドレスをコンソールより設定する必要があります。IP アドレスを設定または変更していない場合は、***Command Line Interface Reference Manual*** の「introduction」、または本マニュアルのセクション 4 を参照してください。

Web ブラウザを使用して IP 設定を変更する場合は Administration フォルダの IP Address メニューを使用します。

スイッチの IP アドレス設定手順:

Administration > IP Address の順でクリックします。以下のように現在の IP アドレスの設定が表示されます。

図 6- 2. IP アドレス設定画面

本スイッチの IP アドレス、サブネットマスク、およびデフォルトゲートウェイを固定設定する方法を説明します。:

1. **Get IP From**ドロップダウンメニューからManualを選択します。
2. **IP Address**、および**Subnet Mask**を入力します。
3. 異なるサブネットから本スイッチにアクセスする場合は、**Default Gateway** の IP アドレスを入力します。同じサブネットからスイッチを管理する場合は、このフィールド内は初期値(0.0.0.0)のままにします。

本スイッチに VLAN 設定をしていない場合は、デフォルトの **VLAN Name** を使用できます。本スイッチは、購入時に VLAN「default」が設定されていて、すべてのポートが所属しています。すでに VLAN 設定をしている場合は、本スイッチにアクセスする管理ステーションに接続しているポートが所属している VLAN の VLAN 名を入力します。ここに表示された VID と同じ VID を持つステーションからのアクセスを許可します。

確認: スイッチの工場出荷時の IP アドレスは 10.90.90.90、サブネットマスクは 255.0.0.0、デフォルトゲートウェイは 0.0.0.0 です。

BOOTPまたはDHCPプロトコルを使用して、IPアドレス、サブネットマスク、およびデフォルトゲートウェイを設定します。:

Get IP From:プルダウンメニューから*BOOTP*または*DHCP*を選択します。次回再起動時のIPアドレスの割り当て方法となります。

IP アドレス 設定オプション:

パラメータ	説明
BOOTP	本スイッチの電源をオンした場合、BOOTP ブロードキャストリクエストを送信します。BOOTP プロトコルは BOOTP サーバによる IP アドレス、ネットマスク、およびデフォルトゲートウェイアドレスの配布を可能とします。このオプションが設定されていると、本スイッチはスイッチに設定済みの IP アドレスではなく、BOOTP サーバに対して IP アドレスを検索します。
DHCP	本スイッチは電源をオンにした場合、DHCP ブロードキャストリクエストを送信します。DHCP プロトコルは DHCP サーバによる IP アドレス、ネットマスク、およびデフォルトゲートウェイアドレスの配布を可能とします。このオプションが設定されていると、本スイッチはスイッチに設定済みの IP アドレスではなく、DHCP サーバに対して IP アドレスを検索します。

Manual	本スイッチの IP アドレス、ネットマスク、およびデフォルトゲートウェイを固定設定します。アドレスはネットワーク管理者によって割り当てられる固有のアドレスを指定します。入力形式：xxx.xxx.xxx.xxx(x は 0 ～ 255 の数字)
Subnet Mask	本スイッチのサブネットを指定します。入力形式：xxx.xxx.xxx.xxx(x は 0 ～ 255 の数字)。クラス A ネットワークには 255.0.0.0、クラス B ネットワークには 255.255.0.0、クラス C ネットワークには 255.255.255.0 を入力します。カスタムサブネットも入力できます。
Default Gateway	この IP アドレスは現在のサブネットの外側に終点アドレスを持つパケットの送信場所を決定します。通常は IP ゲートウェイとして動作するルータまたはホストのアドレスです。ご使用のネットワークがイントラネットの一部ではない場合、またはスイッチがローカルネットワークの外にアクセスさせたくない場合は、このフィールドはそのままにします。
VLAN Name	VLAN 名のエントリをすると、管理ステーションは TCP/IP (Web ブラウザまたは Telnet 経由のインバンド)を使用してスイッチの管理が可能となります。管理ステーションがここでエントリされた VLAN とは別の VLAN に所属していると、その IP アドレスが Security IP Management メニュー内に入力されない限りスイッチの管理をすることはできません。VLAN 設定がまだされていない場合、default VLAN にすべてのスイッチポートが所属します。初期状態では Security IP Management テーブル内にエントリはないため、管理用 VLAN が指定されるまで、または Management Station IP Address が割り当てられるまではスイッチに接続している全管理ステーションがスイッチにアクセスできます。
Auto Config State	Auto Config State が *Enabled*(有効)の場合、スイッチには TFTP 経由で設定ファイルが通知され、自動的に DHCP クライアントになります。設定ファイルは再起動時に実行されます。Auto Config を使用するためには DHCP サーバが設定されて DHCP リレーパケット内に TFTP サーバ IP アドレスと設定ファイル名情報を加える必要があります。TFTP サーバはスイッチからリクエストを受信する場合には、動作中でベースディレクトリ内にリクエストされた設定ファイルを保存しています。クライアントによって使用される設定ファイルの実行に関する情報については DHCP サーバまたは TFTP サーバソフトウェアの説明書を参照してください。(また、TFTP サーバに設定をアップロードする方法については「シングル IP マネージメント設定」セクションを参照ください。) スイッチが自動設定処理を完了しない場合、以前に保存した設定ファイルがスイッチのメモリ内にロードされます。

Applyボタンをクリックし、変更を適用します。

コンソールインタフェースを使用したスイッチのIPアドレス設定

各スイッチに IP アドレスを設定し、それを使用して SNMP ネットワークマネージャや TCP/IP アプリケーション(BOOTP、TFTP など)との通信をします。本スイッチの IP アドレスの初期値は 10.90.90.90 です。デフォルトの IP アドレスはご使用のネットワークアドレス体系に合うように変更してください。

IPアドレスはWebブラウザを使用する設定してください。本スイッチのIPアドレスはBOOTPまたはDHCPプロトコルを使用して自動的に設定することもできます。コンソールポートからCommand Line Interface (CLI)を使用した設定は以下のとおりです。

- コマンドラインプロンプトで**config ipif System ipaddress xxx.xxx.xxx.xxx/ yyy.yyy.yyy.yyy**と入力します。

  (***x***: ***System***という名前のインタフェースに割り当てるIPアドレス、***y***:対応するサブネットマスク)

- **config ipif System ipaddress xxx.xxx.xxx.xxx/z.**と入力することもできます。

  (***x***: ***System***という名前のインタフェースに割り当てるIPアドレス、***z***: CIDR表記によるサブネットマスク数)

管理ステーションが Telnet や Web ブラウザで本スイッチに接続する場合に設定した IP インタフェースを使用します。コマンドが正しく実行されると **"Success"** メッセージが表示されます。

ユーザはこのアドレスを使用して Telnet、Command Line Interface (CLI)、 または Web ブラウザ(GUI)からスイッチの設定や管理ができるようになります。

ポート設定

このセクションにはポート速度を含む各物理ポートのプロパティ設定のための情報があります。**Administration > Port Configuration > Port Settings**の順にメニューをクリックし、以下の画面を表示します。:

Port	State	Speed/Duplex	Flow Control	Connection/Duplex/FlowCtrl	Learning
1	Enabled	Auto	Disabled	100M/Full/None	Enabled
2	Enabled	Auto	Disabled	LinkDown	Enabled
3	Enabled	Auto	Disabled	LinkDown	Enabled
4	Enabled	Auto	Disabled	LinkDown	Enabled
5	Enabled	Auto	Disabled	LinkDown	Enabled
6	Enabled	Auto	Disabled	LinkDown	Enabled
7	Enabled	Auto	Disabled	LinkDown	Enabled
8	Enabled	Auto	Disabled	LinkDown	Enabled
9	Enabled	Auto	Disabled	LinkDown	Enabled
10	Enabled	Auto	Disabled	LinkDown	Enabled
11	Enabled	Auto	Disabled	LinkDown	Enabled
12	Enabled	Auto	Disabled	LinkDown	Enabled
13	Enabled	Auto	Disabled	LinkDown	Enabled
14	Enabled	Auto	Disabled	LinkDown	Enabled
15	Enabled	Auto	Disabled	LinkDown	Enabled
16	Enabled	Auto	Disabled	LinkDown	Enabled
17	Enabled	Auto	Disabled	LinkDown	Enabled
18	Enabled	Auto	Disabled	LinkDown	Enabled

図 6- 3. Port 設定とポート情報テーブル

スイッチポートの設定手順:

1. **From…To…** のプルダウンメニューを使用してポートまたはポートの範囲を選択します。
2. 残りのプルダウンメニューは以下の説明にしたがい設定します。:

パラメータ	説明
State <Enabled>	ポートまたはポートグループの *Enabled*(有効)/*Disabled*(無効)を切り換えて選択します。
Speed/Duplex <Auto>	ポートの Speed(速度)と Duplex/Half-Duplex を切り換えて選択します。*Auto* は 10M/100Mbps、Full/Half duplex でオートネゴシエーションとなります。*Auto* は自動的にポートとポートに接続しているデバイス間を最速な設定にします。 オプションには *Auto*、*10M/Half*、*10M/Full*、*100M/Half*、*100M/Full*、*1000M_M /Full*、*1000M_S /Full*、*1000M/Full* があります。*Auto* 以外のオプションのポート設定は固定となります。 次の3つのタイプ(1000M/Full、1000M_M /Full、1000M_S /Full)のギガビット接続設定ができます。; ギガビット接続はフルデュプレックス接続だけをサポートしており、他の選択肢とは異なる特長を持っています。 1000M_M /Full (マスター)および 1000M_S /Full (スレーブ)パラメータはギガビット接続が可能なスイッチポートと他のデバイス間を 1000BASE-T で結ぶ接続を表しています。マスター設定(1000M_M /Full)によりポートはデュプレックス、速度および物理レイヤタイプに関連する情報を通知することができます。さらに2つの接続している物理レイヤ間のマスターおよびスレーブを決定します。この関係は2つの物理レイヤ間のタイミングコントロールを確立するために必要です。タイミングコントロールはローカルソースによってマスター物理レイヤ上に設定されます。スレーブ設定は(1000M_S /Full)はループタイミングを使用します。マスターから受信したデータストリームよりタイミングをあわせます。一方の接続に 1000M_M /Full を設定するともう一方の接続は 1000M_S /Full に設定される必要があります。それ以外の設定をすると両ポートともリンクダウンとなります。 光ポートは 1000Mbps(フルデュプレックス)固定で、変更できません。Auto または 1000M/Full のみ設定できます。
Flow Control	各ポートのフローコントロール設定を選択します。Full-Duplex では 802.3x フローコントロール、Half-Duplex ではバックプレッシャーによる制御を自動で行います。Enabled(フロー制御あり)または Disabled(フロー制御なし)を選択します。*Auto* は自動的にいずれかを使用します。初期値は *Disabled* (フロー制御なし)です。

Apply ボタンをクリックし、本スイッチに新しい設定を適用します。

ポート種別

ポート種別設定では各ポートに名前をつけることができます。各ポートに名前を割り当てるためには、**Administration > Port Configuration > Port Description** の順にクリックし、以下の画面を表示します。:

図 6- 4. Port Description 設定と Port Description Table

From と **To** のプルダウンメニューを使用し、ポート種別を設定するポートまたはポートの範囲を選択します。続いて Description にポート種別を入力します。

Applyボタンをクリックし、**Port Description Table**内にポート種別を設定します。

エラーによるポートの無効

以下の画面では接続が無効であるポートに関する情報(STPループバック防御のような理由や接続ステータス)を表示します。
Administration > Port Configuration > Port Error Disabledの順でクリックし、以下の画面を表示します。

Port Error Disabled Table

Port	State	Connection	Reason	Description
17	Enabled	Err-Disabled	STP LBD	Port17
19	Enabled	Err-Disabled	STP LBD	
26	Enabled	Err-Disabled	STP LBD	

図 6- 5. Port Error Disabled 画面

以下のパラメータが表示されます。

パラメータ	説明
Port	エラーのために無効になっているポートを表示します。
State	現在のポートのステータス(*Enabled* または *Disabled*)を表示します。
Connection	個別ポートのアップリンク状況(*Enabled* または *Disabled*)を読み出して表示します。
Reason	STP ループバックの発生などポートがエラーによって無効になった理由を表示します。
Description	ポートに設定した名称を表示します。

ユーザアカウント

User Account 画面を使用してユーザの権限を設定します。既存のユーザアカウントを表示するためには **Administration > User Accounts** の順でメニューをクリックし、以下の画面を表示します。

図 6- 6. User Accounts 画面

新しいユーザを追加するために **Add** ボタンをクリックします。既存のユーザの変更または削除のためには該当ユーザの **Modify** ボタンをクリックします。

図 6- 7. User Account Modify Table – 追加

User Name と *New Password* の入力、および新しいパスワードの確認のため同じパスワードを *Confirm New Password* に入力して新しいユーザを追加します。*Access Right* のドロップダウンメニューよりユーザの権限レベル(*Admin* または *User*)を選択します。

図 6- 8. User Account Modify Table – 変更

User Account Modify Table で既存ユーザの変更または削除をします。ユーザアカウントを削除するためには **Delete** ボタンをクリックします。パスワードの変更のためには既存のパスワードを *Old Password* に入力した後、*New Password* に新しいパスワードを入力し、確認のため *Confirm New Password* に再度同じパスワードを入力します。

Apply ボタンをクリックし、変更を有効にします。

Access Right フィールドで権限レベル(*Admin* または *User*) を参照できます。

Show All User Account Entries リンクをクリックし、**User Accounts** 画面に戻ります。

AdminとUser権限

Admin と User の2つのユーザ権限があります。Admin 権限を持つユーザが選択可能なメニューのうちのいくつかは User 権限では使用できません。

Admin と User 権限は以下の表のとおりです。:

表 6- 1. Admin と User 権限

管理	Admin	User
Configuration	○	△
Network Monitoring	○	△
Community Strings and Trap Stations	○	△
Update Firmware and Configuration Files	○	×
System Utilities	○	×
Factory Reset	○	×

ユーザアカウント管理	Admin	User
Add/Update/Delete User Accounts	○	×
View User Accounts	○	×

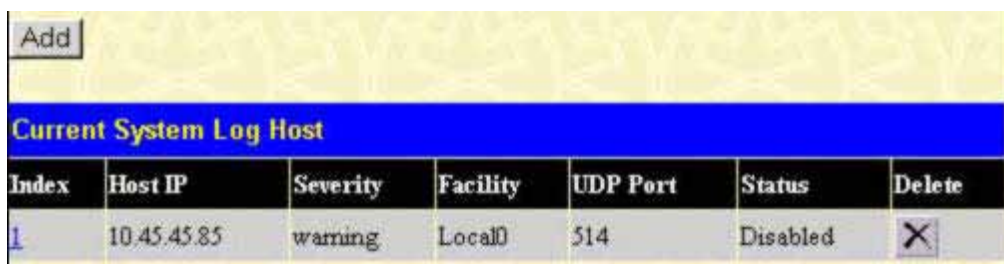
○:使用可能、△:参照のみ、×:使用不可

Admin レベルの権限を持つユーザアカウントを作成後、メインメニューの **Save Changes** 画面を開き、**Save Config** をチェック後、**Apply** ボタンをクリックして変更を保存してください。

ポートミラーリング

本スイッチはポート上で送受信したフレームをコピーし、別のポートに転送します。スニファーや RMON probe のようなモニターデバイスをミラーポートに接続し、最初のポートを通過するパケット情報を参照できます。ネットワーク監視とトラブルシューティングの目的で使用します。**Administration > Port Mirroring** の順でメニューをクリックし、以下の画面を表示します。

表 6- 9. Port Mirroring 画面

ミラーポートの設定手順:

1. **Target Port** ドロップメニューよりフレームをコピーするソースポートとソースポートからのコピーを受信するターゲットポートを選択します。

2. ソースデータの方向を *RX*(受信パケット)、*TX*(送信パケット)、または *Both*(両方)から選択し、**Status** のドロップダウンメニューで本機能を *Enabled*(有効)にします。

3. **Apply** ボタンをクリックし設定を有効にします。

確認: 転送速度の速いポートを遅いポートにミラーリングできません。たとえば、100Mbps ポートからのトラフィックを 10 Mbps ポートにミラーリングしようとすると、スループットの問題が起こります。ソースポートの速度はターゲットポートと同じかそれ以下としてください。また、ターゲットポートはトランクグループに属することはできません。ターゲットポートとソースポートを同じポートにはできません。

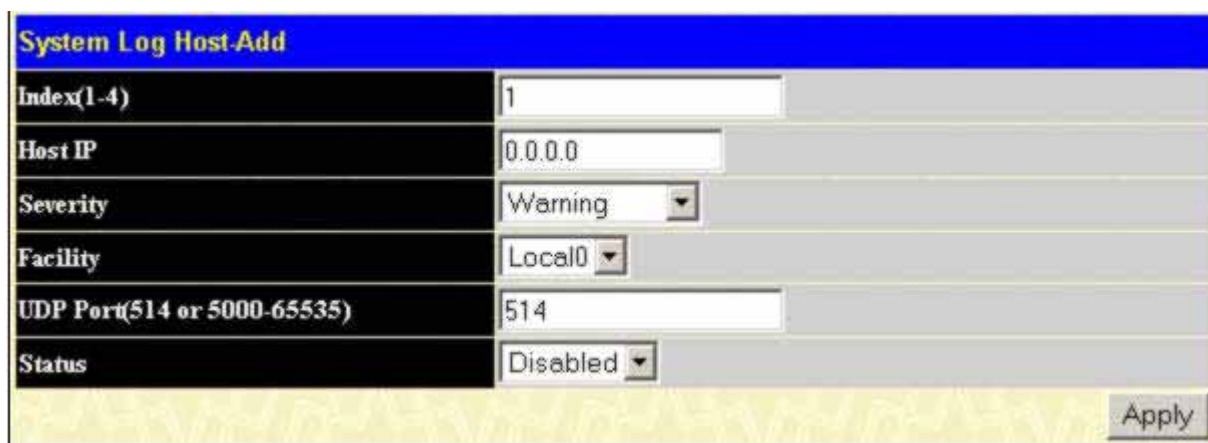
システムログ設定

本スイッチは **Current System Log Host** 画面を使用して Syslog メッセージを最大 4 台のサーバに送信します。**Administration > System Log Settings** 順でメニューをクリックし、以下の画面を表示します。

図 6- 10. Current System Log Host 画面

System Log Server設定の追加と変更のパラメータは同じです。新しくSyslogサーバを追加する場合は**Add**ボタンをクリックします。現在のエントリを編集する場合は、**Index**フィールドのサーバ番号のリンクをクリックします。パラメータの記述については以下の画面を参照してください。

表 6- 11. System Log Host-Add 画面

設定パラメータは以下のとおりです。

パラメータ	説明
Index(1-4)	Syslog サーバ設定インデックス (1-4)
Host IP	Syslog サーバの IP アドレス
Severity	ドロップダウンメニューより送信メッセージのレベルを選択します。オプションは *Warning*、*Informational* および *All* です。

パラメータ	説明	
Facility	オペレーティングシステムデーモンおよびプロセスで Facility 値を割り当てている場合に設定します。Facility を割り当てていないプロセスとデーモンの場合は"*local use*" のいずれかを使用するか、"*user-level*" を使用します。指定できる Facility は以下のとおりです。: 太字で表された Facility 値は、製品の現在の Facility 値であることを意味しています。 **Numerical Code** **Facility**	
	0	kernel messages
	1	user-level messages
	2	mail system
	3	system daemons
	4	security/authorization messages
	5	messages generated internally by syslog line printer subsystem
	7	network news subsystem
	8	UUCP subsystem
	9	clock daemon
	10	security/authorization messages
	11	FTP daemon
	12	NTP subsystem
	13	log audit
	14	log alert
	15	clock daemon
	16	**local use 0 (local0)**
	17	**local use 1 (local1)**
	18	**local use 2 (local2)**
	19	**local use 3 (local3)**
	20	**local use 4 (local4)**
	21	**local use 5 (local5)**
	22	**local use 6 (local6)**
	23	**local use 7 (local7)**
UDP Port (514 or 6000-65535)	Syslog メッセージを送信するために使用する UDP ポート番号を入力します。 初期値は *514* です。	
Status	*Enabled* (有効)または *Disabled* (無効)を選択します。	

Apply ボタンをクリックし設定を有効にします。

Current System Log Server 画面からエントリを削除するためには、削除したい該当エントリの をクリックします。**Current System Log Server** 画面に戻るためには、Show All System Log Servers リンクをクリックします。

SNTP 設定

時刻設定

製品の時刻設定のためには **Administration** > **SNTP Settings** > **Time Setting** の順にクリックし、以下の画面を表示します。

図 6- 12. Current Time: Status 画面

以下のパラメータを設定または表示できます。

パラメータ	説明
Time Settings – Current Time	
Current Time	現在の時刻が表示されます。
Time Source	システムの時刻取得方法が表示されます。
SNTP Settings	
SNTP State	SNTP の *Enabled*(有効) または *Disabled*(無効)をプルダウンメニューから選択します。
SNTP Primary Server	SNTP 情報を取得するプライマリサーバの IP アドレス。
SNTP Secondary Server	SNTP 情報を取得するセカンダリサーバの IP アドレス。
SNTP Poll Interval in Seconds	SNTP 情報の更新リクエストを出す間隔(秒)。
Time Settings – Set Current Time	
Year	システムクロックを更新したい場合に現在の年を選択します。
Month	システムクロックを更新したい場合に現在の月を選択します。
Day	システムクロックを更新したい場合に現在の日を選択します。
Time in HH MM SS	システムクロックを更新したい場合に現在の時刻を時、分、秒で選択します。

Apply ボタンをクリックし、設定を有効にします。

タイムゾーンと DST

SNTPのためのタイムゾーンとDST(Daylight Savings time)を設定します。**Administration** > **SNTP Settings** > **Time Zone and DST** の順にクリックし、以下の画面を表示します。

図 6- 13. Time Zone and DST 設定画面

設定するパラメータは以下のとおりです。:

パラメータ	説明
Time Zone and DST	
Daylight Saving Time State	プルダウンメニューを使用して DST 設定を *Disabled*、*Repeating*、*Annual* から選択します。
Daylight Saving Time Offset in Minutes	プルダウンメニューを使用してローカル DST オフセット(*30*, *60*, *90*, または *120* 分)を構成する時間の量を指定します。
Time Zone Offset : from GMT in +/- HH:MM	プルダウンメニューを使用してグリニッジ時間(GMT)からのローカルタイムのオフセットを指定します。
DST Repeating Settings - Repeating mode を使用して DST 季節時間調整を有効にします。Repeating mode は DST の開始日と終了日を定型で設定します。例: April(4 月)の second week(2 週目)の Saturday(土曜日)に始まり、October(10 月)の last week(最終週)の Sunday(日曜日)に終了することを指定します。	
From Which Week of the Month	DST が始まる月の中の週を *Last*、*First*、*Second*、*Third*、*Fourth* から選択します。
From Which Day of the Week	DST が始まる週の中の曜日を選択します。
From Which Month	DST が始まる月を選択します。
From What Time HH:MM	DST が始まる日の時刻を選択します。

To Which Week	DST が終わる月の中の週を *Last*、*First*、*Second*、*Third*、*Fourth* から選択します。
To Which Day	DST が終わる週の中の曜日を選択します。
To Which Month	DST が終わる月を選択します。
To What Time HH:MM	DST が終わる日の時刻を選択します。
DST Annual Settings - annual mode を使用して DST 季節時間調整を有効にします。Annual mode には DST の開始日と終了日を正確に指定することが要求されます。例：開始日は April 3 で終了日は October 14。	
From What Month	毎年 DST を開始する月を選択します。
From What Date	毎年 DST を開始する日を選択します。
From What Time	毎年 DST を開始する時刻を選択します。
To What Month	毎年 DST を終了する月を選択します。
To What Date	毎年 DST を終了する日を選択します。
To What Time	毎年 DST を終了する時刻を選択します。

Apply ボタンをクリックし、設定を有効にします。

MAC 通知設定

MAC通知は学習し、フォワーディングデータベースに登録されたMACアドレスをモニターするために使用されます。MAC通知を設定するためには、**Administration > MAC Notification Settings** の順にクリックし、以下の画面を表示します。

画面 6- 14. MAC Notification 設定

グローバル設定

次のパラメータの参照または編集ができます。

パラメータ	説明
State	本スイッチ上の MAC 通知をグローバルに *Enabled*(有効)、または *Disabled* (無効)にします。
Interval (1-2147483647)	通知間隔(秒)
History size (1-500)	通知ログリスト内の最大エントリ数。最大 500 まで指定できます。

ポート設定

本スイッチのポートまたはポートグループのMAC通知設定を変更するためには以下のパラメータを設定します。

パラメータ	説明
From…To	プルダウンメニューを使用して MAC 通知を有効/無効にするポートを選択します。
State	選択されたポートの MAC 通知をプルダウンメニューを使用し、*Enabled*(有効)または *Disabled*(無効)にします。初期値は *Disabled* です。

Apply ボタンをクリックし、設定を有効にします。

TFTP サービス

Trivial File Transfer Protocol (TFTP) サービスにより TFTP サーバから本スイッチに新しいファームウェアを転送してアップグレードできます。**Administration > TFTP Services** の順にメニューをクリックし、以下の画面を表示します。**Active** のプルダウンを使用してサービスを選択します。**Download_Firmware** は TFTP プロトコルを使用して外部ソースからスイッチにファームウェアファイルを転送するために使用されます。 **Download_Configuration** は TFTP プロトコルを使用して外部ソースからスイッチに設定ファイルを転送するために使用されます。**Upload_Configuration** は TFTP プロトコルを使用してスイッチから外部ソースにスイッチのログファイルを転送するために使用されます。**Upload_Log** は TFTP プロトコルを使用してスイッチから外部ソースに設定ファイルを転送するために使用されます。実行する操作パラメータを **Active** で選択した後、Server IP Address と File Name を入力し、**Start** ボタンをクリックして転送を開始します。

表 6- 15. TFTP Services 画面

Ping テスト

Ping は指定した IP アドレスに ICMP Echo パケットを送信するプログラムです。受信した機器はその後応答するかまたは本スイッチから送信されたパケットをエコーバックします。スイッチとネットワーク間の接続性を確認するために使用します。

図 6- 16. Ping Test

Target IP Address には ICMP パケットを送付する先の IP アドレスを指定します。**Repeat Pinging for:**には Ping の実行回数(*1～255*)を指定します。**Infinite times** を選択するとプログラムがストップされるまで指定した IP アドレスに ICMP Echo パケットを送り続けます。**Time Out** には Ping パケットの応答待ち時間(*1-99*)を入力します。この時間内に応答パケットを受信しないと未接続と見なします。プログラムを開始するために **Start** ボタンをクリックします。

SNMP マネージャ

SNMP設定

SNMP（簡易ネットワーク管理プロトコル）は OSI 参照モデルの第7層（アプリケーション層）のプロトコルでネットワークデバイスの管理やモニタリングを行います。ネットワーク管理デバイスはSNMPを利用してゲートウェイ、ルータ、そしてその他のネットワークデバイスの設定状態の確認や変更をします。SNMP を利用してシステムの設定を行い、適切なオペレーション、パフォーマンスのモニタリング、デバイスまたはネットワーク全体に潜在する障害検知を行います。

SNMP をサポートする管理デバイスはスイッチ上で動作する SNMP エージェントと呼ばれるソフトウェアを実装しています。SNMP エージェントは管理オブジェクトの変数定義を保持し、デバイスの管理を行います。管理オブジェクトは MIB として定義され、デバイスに実装された SNMP エージェントにより管理される情報表示の基準を（管理側のデバイスに）伝えます。SNMP は MIB（情報管理ベース）仕様およびネットワークを介して（管理デバイスに）送信される際のプロトコルのフォーマットを定義しています。

DES-3000 シリーズは SNMP のバージョン 1（SNMP v1）、2c（SNMP v2c）、および 3（SNMP v3）をサポートしています。この3種類の SNMP により管理側とネットワークデバイス間のセキュリティレベルを調整します。

SNMP v1 および v2c では、ユーザ認証において SNMP コミュニティ名をパスワードのように利用します。リモートユーザ SNMP（エージェント）と（管理側の）デバイスは同一のコミュニティ名に所属している必要があります。認証されないメッセージは破棄されます。

SNMP の v1 または v2c（のデバイスや管理ソフト）のデフォルトで設定されているコミュニティ名は次のとおりです。

- **public** - （ネットワークデバイスSNMP管理ソフトに）MIBオブジェクトの読み出し権限が許可されているコミュニティ名です。
- **private** - MIBオブジェクトの読み出しと書き込みの権限を与えられているコミュニティ名です。

SNMP v3 では（旧バージョンより）2 種類の拡張された認証プロセスがあります。それらは、SNMP マネージャとしてのユーザリストとユーザ属性の機密性維持することと、リスト上のユーザごとに SNMP マネージャとしてのアクセス制限を設定できることです。

ネットワークデバイスはリスト上のユーザに対してアクセス制限を定義します。（対応する）SNMP のバージョンは SNMP マネージャのグループごとに設定されます。よって、読み取り権限の定義、または SNMP v1 を使用したトラップ受信を可能にした SNMP マネージャグループと SNMP v3 を利用した読み取りと書き込みの権限を付与したグループの作成をグループごとに作成できます。

SNMP v3 を利用して個々のユーザや SNMP の管理グループは特定の SNMP 管理機能の実行や制限を設定できます。SNMP 管理機能は特定の MIB に関連した MIB オブジェクトである OID を利用して許可／拒否を定義します。SNMP v3 の設定の詳細は次項をご覧ください。

MIB(管理情報ベース)

ネットワークデバイスに実装された MIB(情報管理ベース)にはデバイスの管理情報を格納しています。ネットワークデバイスは標準的なネットワークデバイス管理情報として MIB-Ⅱをサポートしています。MIB オブジェクト（と呼ばれるデバイスの情報）の値を SNMP 管理ソフトにより取得します。本スイッチは標準的な MIB-Ⅱに加えて拡張 MIB を実装しています。OID と呼ばれる MIB オブジェクトの識別子を定義することで拡張 MIB の情報を取得します。MIB の値は読み取り専用ともの と、読み取りと書き込みが可能なものがあります。

DES-3000 シリーズはネットワーク環境に対して柔軟に対応できる SNMP 管理機能を搭載しています。SNMP 管理機能はカスタマイズされネットワークの管理における管理者の要求に対応しています。SNMP v3 メニューにより SNMP のバージョンを目的に応じて選択できます。

さらに簡易ネットワークプロトコルである SNMP のバージョン 1、2c、および 3 をサポートします。ネットワーク管理者は管理するデバイスにあわせて SNMP のバージョンを定義できます。この3種類の SNMP により管理側とネットワークデバイス間のセキュリティレベルを調整します。

SNMP 設定は Web マネージャにある SNMP v3 フォルダのメニューにより変更できます。ネットワーク上の SNMP にデバイスへのアクセスを許可されているワークステーションは Management Station IP Address メニューによりアクセス制限が可能です。

SNMP ユーザテーブル

SNMP User Table は（SNMP 管理）デバイスで設定されているすべての SNMP ユーザを表示します。

Administration > SNMP Manager > SNMP User Table の順にクリックし、以下の画面を表示します。

Add

Total Entries:1 (Note: It is allowed insert 10 entries into the table only.)

SNMP User Table

User Name	Group Name	SNMP Version	Delete
initial	initial	V3	✕

図 6- 17. SNMP User Table

User Name（ユーザ名）を削除するためには **Delete** 欄の ボタンをクリックします。

ユーザ名登録情報の詳細を確認するためには該当する**User Name**のリンクをクリックし、次の**SNMP User Table Display**画面を表示します。

SNMP User Table Display

User Name	initial
Group Name	initial
SNMP Version	V3
Auth-Protocol	None
Priv-Protocol	None

Show All SNMP User Table Entries

図 6- 18. SNMP User Table Display

次のパラメータが表示されます。:

パラメータ	説明
User Name	SNMP ユーザ名。(32 文字までの半角英数字)
Group Name	SNMP のグループを認識する名前。SNMP メッセージのリクエストにも使用します。
SNMP Version	*V1* - SNMP バージョン 1 を使用しています。 *V2c* - SNMP バージョン 2 を使用しています。 *V3* - SNMP バージョン 3 を使用しています。
Auth-Protocol	認証プロトコルです。 *None* - 認証のプロトコルは使用されていません。 *MD5* - HMAC-MD5-96 メッセージ認証方式を使用します。 *SHA* - HMAC-SHA 認証方式を使用します。
Priv-Protocol	暗号化プロトコルです。 *None* – 暗号化は使用されていません。 *DES* - DES-56-bit の共通鍵暗号方式である DES-CBS（Data Encryption Standard - Cipher Block Chaining）暗号化を使用しています。

SNMP User Table画面に戻るには、Show All SNMP User Table Entries リンクをクリックします。**SNMP User Table Configuration**に新しくエントリを追加する場合には、**SNMP User Table**画面で**Add**ボタンをクリックし、以下の**SNMP User Table Configuration**画面を表示します。

図 6- 19. SNMP User Table Configuration 画面

次のパラメータを設定することができます。:

パラメータ	説明
User Name	SNMPユーザ名を入力します。(32文字までの半角英数字)
Group Name	SNMPのグループを認識する名前。SNMPメッセージのリクエストにも使用します。
SNMP V3 Encryption	**encrypted**フィールドをチェックするとSNMP V3 暗号化を有効にします。SNMP V3 モードのみ有効です。以下の2つのフィールドに暗号sを設定できます。
Auth-Protocol	*MD5* - HMAC-MD5-96メッセージ認証方式を使用する場合に指定します。このフィールドはSNMP Versionで*V3*が選択され、**encrypted**がチェックされている場合に使用できます。さらにパスワードを入力します。 *SHA* - HMAC-SHA 認証方式を使用する場合に指定します。このフィールドはSNMP Versionで*V3*が選択され、**encrypted**がチェックされている場合に使用できます。さらにパスワードを入力します。
Priv-Protocol	*None* -認証のプロトコルは使用されていません。 *DES* - DES-CBS(DES-56)をベースとしたDES-56-bit暗号方式を使用する場合に指定します。このフィールドはSNMP Versionで*V3*が選択され、**encrypted**フィールドがチェックされている場合に使用できます。このフィールドはパスワード(8～16文字の半角英数字)をユーザに要求します。

パラメータ入力後、**Apply** ボタンをクリックし、設定を有効にします。SNMP User Table に戻るためには、Show All SNMP User Table Entries リンクをクリックします。

SNMP ビューテーブル

SNMP View Table ではビューに対するサブツリーを割り当てます。これにより SNMP マネージャがアクセスできる MIB オブジェクトを定義できます。**Administration > SNMP Manager > SNMP View Table** の順にクリックし、以下の **SNMP View Table** を表示します。:

Add

Total Entries:8 (Note: It is allowed insert 30 entries into the table only.)

SNMP View Table

View Name	Subtree	View Type	Delete
restricted	1.3.6.1.2.1.1	Included	X
restricted	1.3.6.1.2.1.11	Included	X
restricted	1.3.6.1.6.3.10.2.1	Included	X
restricted	1.3.6.1.6.3.11.2.1	Included	X
restricted	1.3.6.1.6.3.15.1.1	Included	X
CommunityView	1	Included	X
CommunityView	1.3.6.1.6.3	Excluded	X
CommunityView	1.3.6.1.6.3.1	Included	X

図 6- 20. SNMP View Table

SNMP View Table のエントリを削除する場合は、**Delete** 欄の ボタンをクリックします。新規に登録する場合は **Add** ボタンをクリックし、登録画面を表示します。

SNMP View Table Configuration

View Name	
Subtree OID	
View Type	Included

Apply

Show All SNMP View Table Entries

図 6- 21. SNMP View Table Configuration 画面

本テーブルで作成された SNMP グループは、**SNMP User Table** の SNMP ユーザと前の画面で作成したビューを割り当てます。

次のパラメータを設定します。:

パラメータ	説明
View Name	ビュー名(32 文字までの半角英数字)を入力します。ビュー名は作成する SNMP ビューに使用されます。
Subtree OID	ビューに対するサブツリーの OID を入力します。OID は SNMP により情報取得のために SNMP エージェントに要求される MIB オブジェクトの識別子です。
View Type	ビュータイプです。Subtree OID で選択した MIB オブジェクトを SNMP からの要求に対してトラップ通知に含めるかどうかを指定します。*Included* を選択するとトラップに OID で指定したオブジェクトは通知され、*Excluded* を選択するとトラップ通知には含まれません。

Apply ボタンをクリックし、新しい設定を登録します。**SNMP View Table** に戻るには、Show All SNMP View Table Entries リンクをクリックします。

SNMP グループテーブル

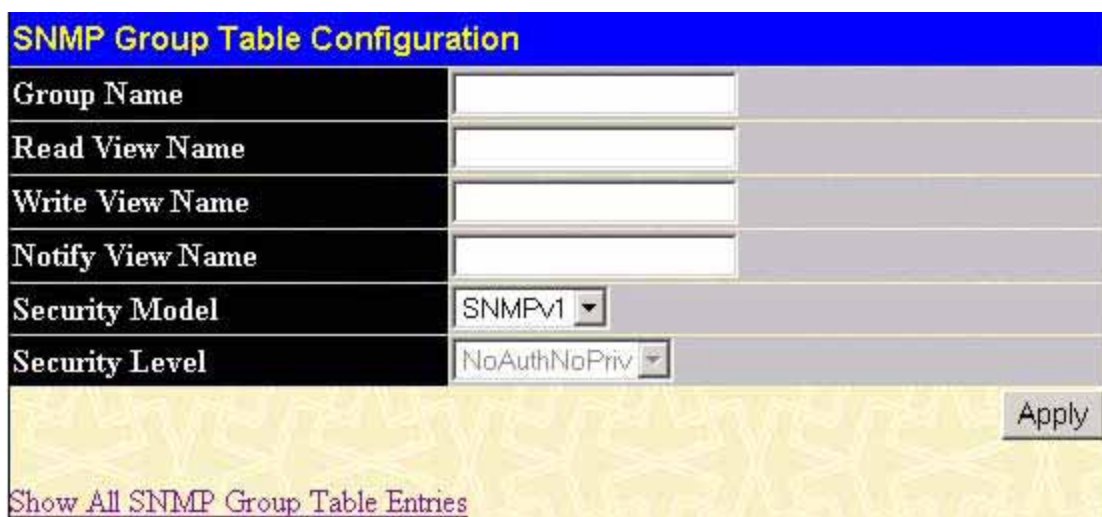
ここで作成する SNMP グループは **SNMP User Table** の SNMP ユーザと直前のメニューで作成したビューを割り当てます。**Administration > SNMP Manager > SNMP Group Table** とクリックし、以下の **SNMP Group Table** 画面を表示します。:

Add

Total Entries:10 (Note: It is allowed insert 30 entries into the table only.)

SNMP Group Table

Group Name	Security Model	Security Level	Delete
g1	SNMPv3	NoAuthNoPriv	X
public	SNMPv1	NoAuthNoPriv	X
public	SNMPv2	NoAuthNoPriv	X
initial	SNMPv3	NoAuthNoPriv	X
private	SNMPv1	NoAuthNoPriv	X
private	SNMPv2	NoAuthNoPriv	X
ReadGroup	SNMPv1	NoAuthNoPriv	X
ReadGroup	SNMPv2	NoAuthNoPriv	X
WriteGroup	SNMPv1	NoAuthNoPriv	X
WriteGroup	SNMPv2	NoAuthNoPriv	X

図 6- 22. SNMP Group Table

SNMP Group Table よりエントリ情報を削除するには **Delete** 欄の ボタンをクリックします。

SNMP Group Table に登録されているエントリの設定を表示するには **Group Name** にあるエントリのリンクをクリックします。

SNMP Group Table Display

Group Name	public
Read View Name	CommunityView
Write View Name	
Notify View Name	CommunityView
Security Model	SNMPv1
Security Level	NoAuthNoPriv

Show All SNMP Group Table Entries

図 6- 23. SNMP Group Table Display – 参照画面

SNMP Group Table に新しいエントリを追加するには**SNMP Group Table**画面左上の**Add**ボタンをクリックし、以下の**SNMP Group Table Configuration**画面を表示します。

図 6- 24. SNMP Group Table Configuration – 追加画面

次のパラメータを設定します。

パラメータ	説明
Group Name	SNMP グループまたはユーザを認識する名前を入力します。(32 文字までの半角英数字)
Read View Name	SNMP メッセージを要求する SNMP グループ名を入力します。
Write View Name	SNMP エージェントに書き込み権限を与える SNMP グループ名を入力します。
Notify View Name	SNMP エージェントによるトラップメッセージを送信する SNMP グループ名を入力します。
Security Model	SNMP バージョンをプルダウンメニューより選択します。 *SNMPv1* - SNMP バージョン 1 を使用する場合に選択します。 *SNMPv2* - SNMP バージョン 2c を使用する場合に選択します。SNMPv2 は効率化と高機能化をサポートし、MIB オブジェクトの枠組みを定めている SMI（情報管理の構造）の改良とセキュリティ仕様を拡張しています。 *SNMPv3* - SNMP バージョン 3 を使用する場合に選択します。SNMPv3 ではネットワークデバイスに対して認証と暗号化によるアクセス制御が行えます。
Security Level	SNMPv3 を使用する場合のセキュリティレベルをプルダウンメニューより選択します。 • *NoAuthNoPriv* – SNMP マネージャと SNMP エージェント間の通信において認証や暗号化は行いません。 • *AuthNoPriv* – SNMP マネージャと SNMP エージェント間の通信において認証が必要ですが暗号化による通信は行われません。 • *AuthPriv* – SNMP マネージャと SNMP エージェント間の通信において認証が必要で暗号化による通信を行います。

Apply ボタンをクリックし、新規登録を追加します。**SNMP Group Table** 画面に戻るには、Show All SNMP Group Table Entries リンクをクリックします。

SNMP コミュニティテーブル設定

SNMP コミュニティテーブルを利用して SNMP マネージャと SNMP エージェントの関係を定義した SNMP コミュニティ名を作成します。コミュニティ名は SNMP エージェントに接続する際のパスワードとして使用され、次の特長があります。

- アクセスリストの SNMP マネージャの IP アドレスをコミュニティ名として使用して SNMP エージェントへのアクセスに利用できること
- すべての MIB オブジェクトの構成を定義する MIB ビューへのアクセスが可能であること
- 読み出しおよび書き込み権限、または読み出しのみの権限を定義された MIB へのアクセスが可能なこと

SNMP コミュニティエントリを設定するには、**Administration > SNMP Manager > SNMP Community Table** の順にクリックし、以下の画面を表示します。：

図 6- 25. SNMP Community Table 画面

次のパラメータを設定します。

パラメータ	説明
Community Name	コミュニティ名。SNMP コミュニティ名を 32 文字までの半角英数字で入力します。コミュニティ名はパスワードのような役割をし、SNMP マネージャが SNMP エージェントの MIB オブジェクト（MIB 変数）にアクセスする際に使用されます。
View Name	ビュー名。ビュー名を 32 文字までの半角英数字で入力します。ビュー名は SNMP マネージャが SNMP エージェントの MIB オブジェクトにアクセスするときに利用します。ビュー名は、SNMP View Table に登録されている必要があります。
Access Right	アクセス権限。 *Read Only* - SNMP コミュニティ名は MIB オブジェクトに対して読み出し権限のみ与えられています。 *Read Write* - SNMP コミュニティ名は MIB オブジェクトに対して読み出しと書き込みの権限を与えられています。

Apply ボタンをクリックし、新しいコミュニティを追加します。**SNMP Community Table** より登録情報を削除する場合は、削除する Community Name の **Delete** 欄の ボタンをクリックします。

SNMP ホストテーブル

SNMP Host Table 画面を利用して SNMP のトラップ送信先（の IP アドレス）を登録します。

Administration > SNMP Manager > SNMP Host Table の順にクリックし、以下の **SNMP Host Table** 画面を表示します。

登録した情報を削除するには **Delete** 欄の ボタンをクリックします。

SNMP Host Table に登録されているエントリの現在の設定を表示するには **Host IP Address** 欄のエントリのリンクをクリックします。

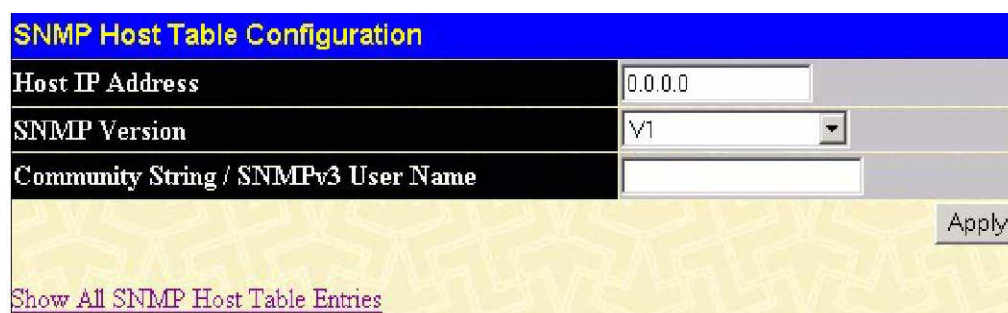



図 6- 26. SNMP Host Table

SNMP Host Tableに新規登録するには、**SNMP Host Table**画面左上の**Add**ボタンをクリックします。以下の**SNMP Host Table Configuration**画面が表示されます。

図 6- 27. SNMP Host Table Configuration 画面

次のパラメータを設定します。

パラメータ	説明
Host IP Address	ホスト IP アドレス。SNMP 管理ホストとして使用する遠隔操作デバイスの IP アドレスを入力します。
SNMP Version	SNMP バージョン。 *V1* - SNMP バージョン 1 を使用する場合に選択します。 *V2c* - SNMP バージョン 2 を使用する場合に選択します。 *V3-NoAuth-NoPriv* - SNMP バージョン 3 を NoAuth-NoPriv security level として使用する際に選択します。 *V3-Auth-NoPriv* - SNMP バージョン 3 を Auth-NoPriv security level として使用する際に選択します。 *V3-Auth-Priv* – SNMP バージョン 3 を Auth-Priv security level として使用する際に選択します。
Community String / SNMPv3 User Name	コミュニティ名または SNMP v3 ユーザ名を入力します。

Apply ボタンをクリックし、新規設定を行います。**SNMP Host Table** に戻るためには Show All SNMP Host Table Entries リンクをクリックします。

SNMP エンジン ID

Engine ID は SNMP v3 で使用される識別名です。識別名は英数小文字で表記され、ネットワークデバイスの識別に使用されます。SNMP Engine ID を表示するためには **Administration > SNMP Manager > SNMP Engine ID** の順にクリックし、以下の **SNMP Engine ID** 画面を表示します。

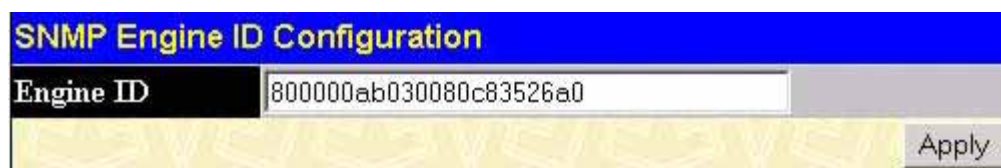



図 6- 28. SNMP Engine ID Configuration 画面

Engine ID を変更するためには新しい Engine ID を入力し、**Apply** ボタンをクリックします。

IP-MAC バインディング

IP ネットワークレイヤは 4 バイトのアドレス、イーサネットリンクレイヤは 6 バイトの MAC アドレスを使用します。これらの2つのアドレスタイプをバインディングするとレイヤ間のデータ転送が可能になります。IP-MAC バインディングの第一の目的はスイッチにアクセスするユーザ数を制限することです。認証済みのクライアントだけが IP-MAC アドレスのペアを設定済みのデータベースと調合することでスイッチポートにアクセスできます。未認証のユーザが IP-MAC バインディングが有効なポートにアクセスしようとすると、システムはパケットを破棄することでアクセスをブロックします。IP-MAC バインディングエントリの最大数はチップの性能(例：ARP テーブルサイズ)とデバイスのストレージサイズによって異なります。IP-MAC バインディングエントリの最大数は 500 です。認証ユーザは CLI または Web ブラウザで設定します。機能はポートベースであり、各ポートごとにこの機能を有効または無効にすることができます。

IP-MACバインディングポート

IP-MAC Ports Settings メニューでポートごとに IP-MAC バインディング設定を行うことができます。有効になったポートはポートへのイングレスパケットに IP-MAC チェックを適用します。チェックに使用される IP-MAC データベースは **IP-MAC Binding Table** とともに設定する必要があります。(以下参照。)

指定ポートで IP-MAC バインディングを有効/無効にするためには **Administration > IP-MAC Binding > IP-MAC Binding Port** の順にクリックし、**IP-MAC Binding Ports Setting** 画面を表示します。**From** と **To** フィールドでポートまたはポートの範囲を選択します。**State** フィールドでポートの有効/無効を設定し、**Apply** ボタンをクリックし、設定を保存します。

図 6- 29. IP-MAC Binding Ports 画面

IP-MAC バインディングポートが有効である場合、use the IP-MAC Binding メニューを使用して IP-MAC バインディングを有効なポートに設定します。

IP-MACバインディングテーブル

以下の画面で IP-MAC バインディングエントリを作成します。**Administration > IP-MAC Binding > IP-MAC Binding Table** の順にクリックし、**IP-MAC Binding Setting** 画面を表示します。対応するフィールドに許可するユーザの IP および MAC アドレスを入力し、**Add** ボタンをクリックします。特定のポートで IP-MAC バインディングチェックを使用するためには、**IP-MAC Binding Ports Setting** メニューではじめにポートを Enabled(有効)にする必要があります(上図参照)。ポートは **Port** フィールドに数字の範囲(例:"1-3")で指定するか、**All** オプション(すべてのポート)を選択します。

図 6- 30. IP-MAC Binding Table メニュー

バインディングエントリの IP アドレスまたは MAC アドレスを変更する場合はフィールド変更後に **Modify** ボタンをクリックします。IP-MAC バインディングエントリを検索するためには IP と MAC アドレスを入力し、**Find** ボタンをクリックします。エントリを削除するためには **Delete** 欄の✕をクリックします。テーブルからすべてのエントリを削除する場合は **Delete All** ボタンをクリックします。

IP-MACバインディングブロック

IP-MACバインディング制限によってブロックされた未承認のデバイスを参照するためには**Administration > IP-MAC Binding > IP-MAC Binding Blocked** の順にクリックし、**IP-MAC Binding Blocked** 画面を表示します。

図 6- 31. IP-MAC Binding Blocked 画面

IP-MAC バインディング制限によってブロックされた未認証デバイスを検索するためには、**VLAN Name** と **MAC Address** を入力し、**Find** ボタンをクリックします。エントリを削除するためにはエントリの MAC アドレス隣の✕ ボタンをクリックします。テーブルからすべてのエントリを削除する場合は **Delete All** ボタンをクリックします。

D-Link シングル IP マネージメント

Single IP Management (SIM) 概要

D-Link Single IP Management とはスタックポートまたはモジュールを使用する代わりにイーサネット経由でスイッチをスタックする方法です。"Single IP Management" 機能には以下の長所があります。:

1. SIMは大きなネットワークの帯域要求の増加に対応しながら小ワークグループやワイアリングクローゼットを簡単に管理することができます。
2. SIMはご使用のネットワークに必要なIPアドレス数を軽減します。
3. SIMはスタック技術を使用する場合にスタック接続のための特別なケーブルをなくし、ご使用のトポロジーオプションを制限する距離のバリアを排除します。

D-Link Single IP Management (以下 SIM と呼ぶ) を使用したスイッチにはさらに以下の規則があります。:

- SIM は本スイッチのオプション機能で CLI または Web ブラウザ経由で簡単に有効/無効にできます。SIM グループはご使用のネットワーク内でスイッチの操作に影響を与えることはありません。
- SIM を使用する 3 つのクラシフィケーションがあります。***Commander Switch (CS)***はグループのマスタースイッチ、***Member Switch (MS)***は CS によって SIM グループのメンバとして認識されるスイッチ、***Candidate Switch (CaS)*** は SIM グループに物理的にリンクはしているが、SIM グループのメンバとして認識されていないスイッチです。
- SIM グループは Commander Switch (CS)をひとつだけ持つことができます。
- 特定の SIM グループ内のすべてのスイッチは同じ IP サブネット(ブロードキャストドメイン)内にある必要があります。
- SIM グループには Commander Switch (番号:0)を含み、最大 33 個のスイッチ(番号:1-32)まで受け入れ可能です。
- 同じ IP サブネット内の SIM グループ数に制限はありませんが、1つのグループにしか所属することはできません。
- マルチプル VLAN が設定されていると SIM グループはスイッチ上のデフォルト VLAN だけを使用します。
- SIMはSIMをサポートしていないデバイスを経由することができます。そのためCSから1個以上はなれたスイッチを管理することができます。

SIM グループは 1 かたまりとして管理されるスイッチのグループです。SIM スイッチは 3 つの異なる役割を持つことができます。:

1. **Commander Switch (CS)** - グループの制御デバイスとして手動で設定されるスイッチで、以下の特長を持っています。:

   ・IP アドレスを持っています。

   ・別のシングル IP グループの CS または MS ではない。

   ・マネージメント VLAN 経由で MS に接続します。

2. **Member Switch (MS)** - シングルIPグループに参加し、CSからアクセス可能なスイッチです。以下の特長を持っています。:

   ・別の IP グループの CS または MS ではない。

   ・CS マネージメント VLAN 経由で CS に接続可能です。

3. **Candidate Switch (CaS)** - SIMグループに参加する準備が整っているが、MSではないスイッチです。CaSはSIMグループのMSになるために手動設定でxStack DGS-3400シリーズスイッチのSIMグループに参加することができます。CaSとして設定したスイッチはSIMグループのメンバではなく、以下の特長を持っています。:

   ・別のシングル IP グループの CS または MS ではない。

   ・CS マネージメント VLAN 経由で CS に接続することができます。

SIM グループの CS として本スイッチを設定後、追加のスイッチは CS に直接接続することで MS としてグループに参加できます。CS だけが SIM に有効な CaS に対してエントリを許可します。CS はその後 MS へのアクセスのためにインバンドエントリポイントとして動作します。CS の IP アドレスがグループのすべての MS への経路になり、CS の管理パスワードや認証は SIM グループのすべての MS へのアクセスを制御します。

SIM が有効の場合、CS 内のアプリケーションはパケットの行き先を変えます。アプリケーションは管理者からのパケットを復号化し、データを編集後、MS に送信します。実行後、CS は MS から応答を受信し、符号化して管理者に戻します。

CaS が MS になる場合、自動的に CS が所属する最初の SNMP コミュニティ(リード権/ライト権、リード権だけを含む)のメンバになります。しかし、MS が自身の IP アドレスを持つ場合、CS を含むグループ内の他のスイッチが所属しない SNMP コミュニティに所属できます。

Webインタフェースを使用したSIM

すべてのスイッチが工場出荷時設定で Candidate (CaS)スイッチとして設定され、Single IP Management は無効です。Web ブラウザを使用してスイッチの SIM を有効にするためには **Administration > Single IP Setting > SIM Settings** の順にクリックし、以下の画面を表示します。

図 6- 32. SIM Settings 画面(無効)

プルダウンメニューで**SIM State** を *Enabled* (無効)にし、**Apply**ボタンをクリックします。画面はリフレッシュして以下の**SIM Settings** 画面が表示されます。

図 6- 33. SIM Settings 画面(有効)

次のパラメータを設定します。:

パラメータ	説明
SIM State	プルダウンメニューでスイッチの SIM 機能を有効または無効にします。*Disabled* はスイッチの SIM 機能を無効にします。
Role State	プルダウンメニューでスイッチの SIM の役割を変更します。2つから選択できます。 *Candidate* - Candidate Switch (CaS)は SIM グループのメンバではないが、Commander Switch(CS)に接続します。本スイッチの SIM 機能の初期設定です。 *Commander* – このパラメータを選択するとスイッチを Commander Switch(CS)にします。このスイッチに他スイッチが SIM グループのメンバとしてイーサネット経由で参加します。このオプションを選択し、スイッチの SIM 設定を有効にします。
Discovery Interval	スイッチが Discovery パケットを送付する Discovery プロトコル間隔(秒)を設定します。CS への返信情報には接続の他のスイッチ(例:MS、CaS)の情報を含んでいます。*30～90* (秒)で指定します。

Holdtime	Discovery Interval を利用して他のスイッチから受信した情報を保持する時間(秒)を設定します。(*100～255* 秒)

Apply ボタンをクリックし、設定を適用します。CS を有効にすると、**Single IP** フォルダの Web 経由で SIM 設定をサポートする **Topology**、 **Firmware Upgrade**、**Configuration Backup/Restore** および **Upload Log** のリンクを使用できます。

トポロジー

Topology 画面は SIM グループ内のスイッチの設定および管理に使用されます。本画面は表示のためにはご使用のコンピュータに Java スクリプトが必要です。

ご使用のサーバ上の Java ランタイム環境を初期化する必要があります。Topology メニューをクリックし、以下のトポロジー画面を表示します。

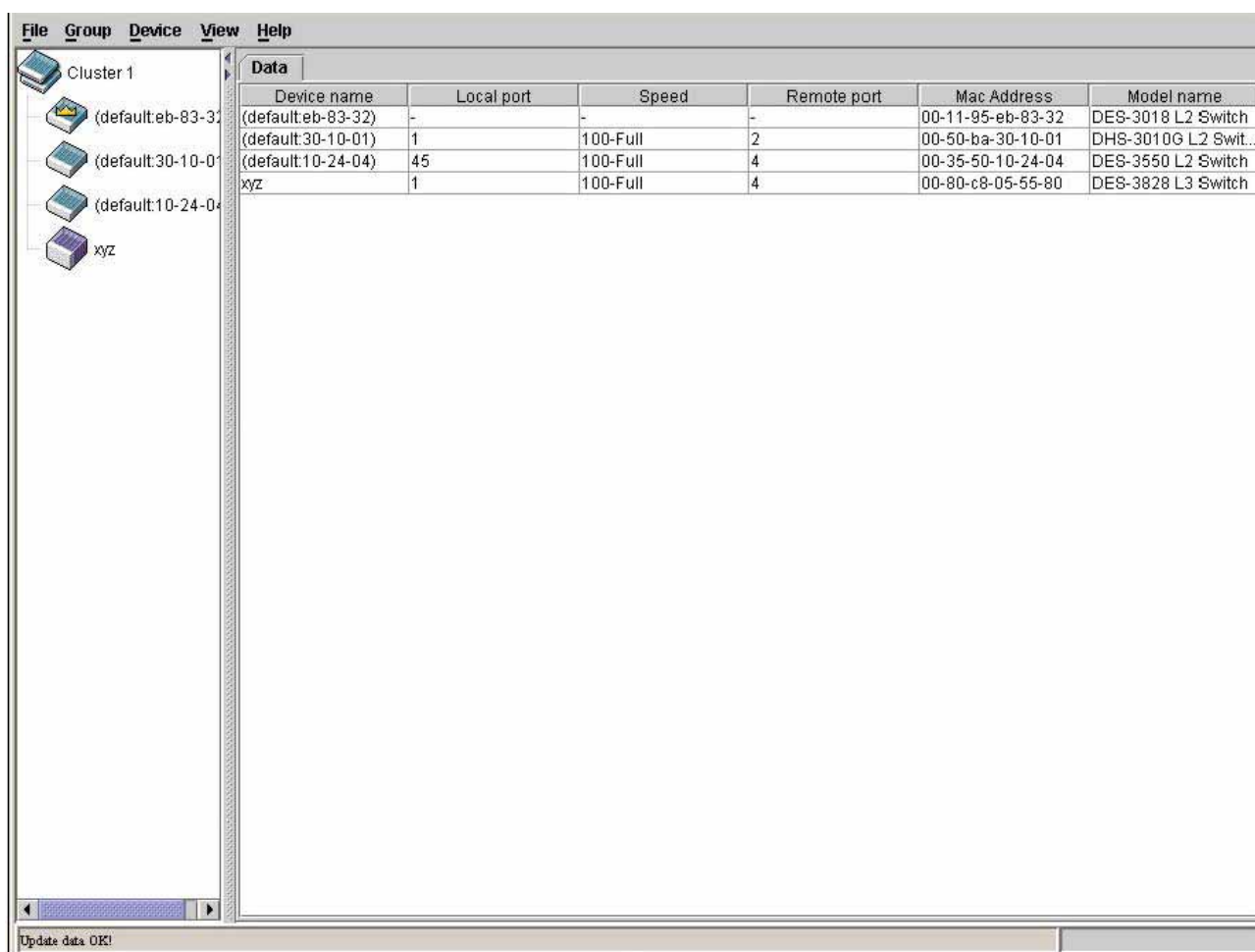



図 6- 34. Single IP Management 画面 - ツリー表示

ツリー表示画面のDataタブには以下の情報があります。

パラメータ	説明
Device name	ユーザが設定した SIM グループ内のスイッチのデバイス名が表示されます。デバイス名がない場合は Default が与えられ、識別のために MAC アドレスの終わり 6 文字が付加されます。
Local port	MS または CaS が接続している CS 上の物理ポート数を表示します。 CS はこのフィールドにはエントリを持ちません。

Speed	CS とMS、または CaS 間の接続速度を表示します。
Remote port	CS が接続している MS または CaS 上の物理ポート数を表示します。CS はこのフィールドにエントリを持ちません。
MAC Address	対応するスイッチの MAC アドレスを表示します。
Model name	対応するスイッチの製品名を表示します。

Topology Mapを参照するためにはツールバーの**View** メニューで**Topology**をクリックし、以下の画面を表示します。**Topology View** は定期的に(初期値:20秒) リフレッシュします。

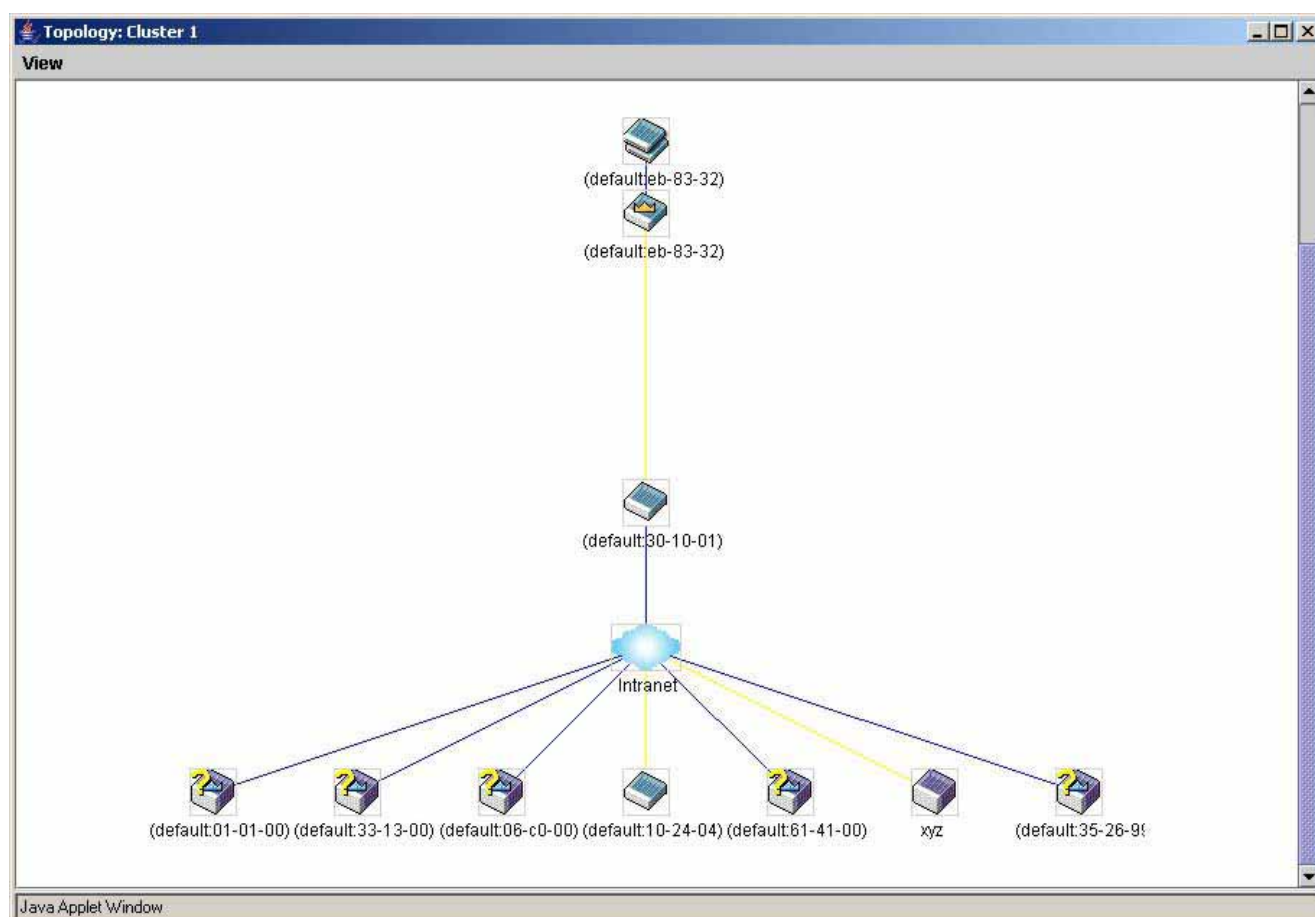



図 6- 35. Topology view

この画面は SIM グループ内のデバイスが他のグループおよび他のデバイスとどのように接続しているかを表示します。この画面で表示されるアイコンは以下のとおりです。

アイコン	説明
	グループ
	Layer 2 Commander Switch
	Layer 3 Commander Switch
	他のグループのCommander Switch(CS)

	Layer 2 Member Switch.
	Layer 3 Member Switch
	他のグループのMember Switch(MS)
	Layer 2 Candidate Switch
	Layer 3 Candidate Switch
	不明なスイッチ
	SIMではないデバイス

Tool Tips

Topology 参照画面ではマウスが設定とデバイス情報の参照のために重要な役割を果たします。トポロジー画面内の特定のデバイス上にマウスカーソルを指定すると、ツリービュー上にある特定のデバイスについて以下のように情報をツールチップで表示します。

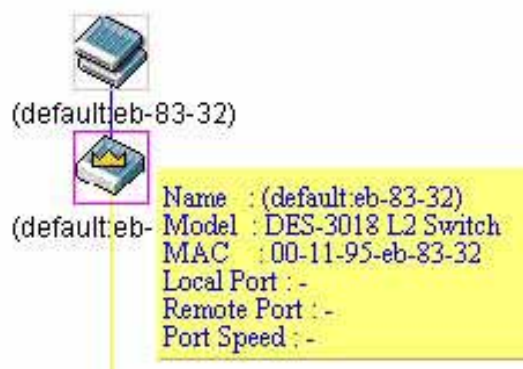



図 6- 36. Tool Tip を利用したデバイス情報

2つのデバイス間を結ぶ線にマウスカーソルを指定すると以下のとおりそのデバイス間の接続速度がツールチップに表示されます。

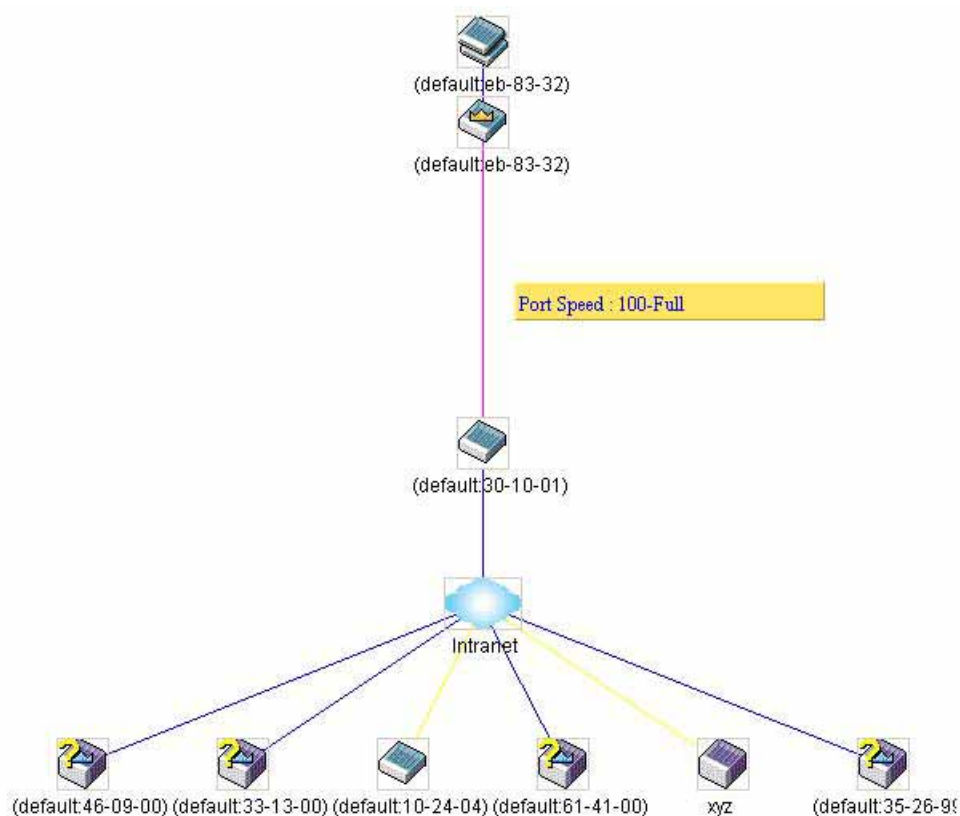



図 6- 37. Tool Tip を利用したポート速度表示

右クリックメニュー

デバイス上でマウスを右クリックするとSIMグループの機能とアイコンに割り当てられたメニューを選択できます。

グループアイコン

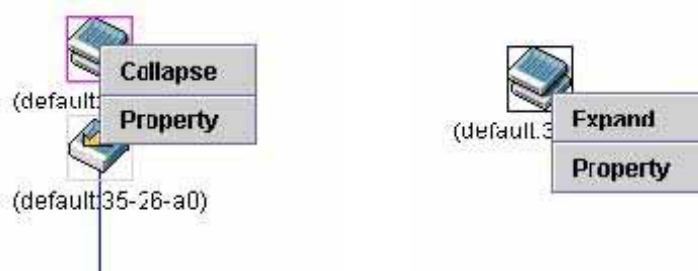



図 6- 38. グループアイコンを右クリックした例

以下のオプションが表示されます。:

- **Collapse** - シングルアイコンによって表示されるグループをまとめます。
- **Expand** - SIM グループを展開します。
- **Property** - グループ情報をポップアップ画面で表示します。

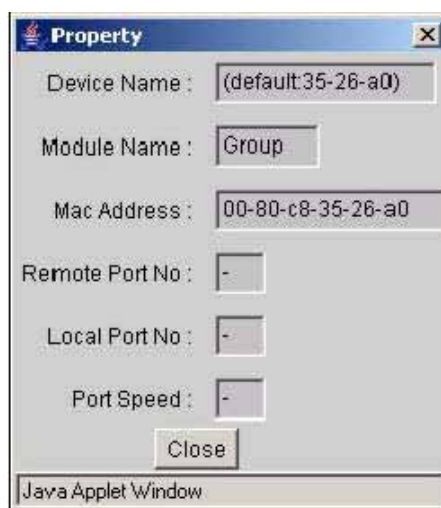



図 6- 39. Property 画面

Commander Switch アイコン

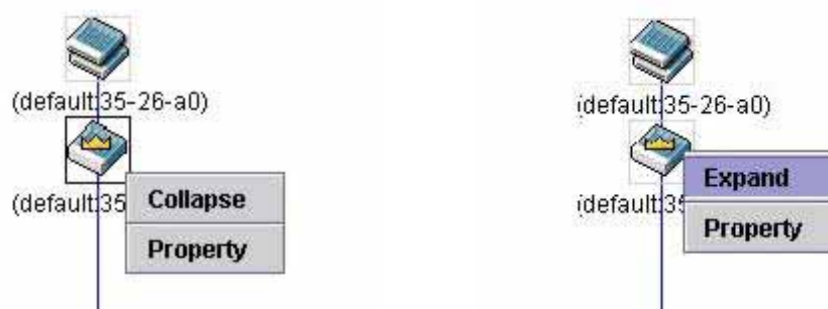



図 6- 40. Commander アイコンを右クリックした例

以下のオプションが表示されます。:

- **Collapse** - シングルアイコンによって表示されるグループをまとめます。
- **Expand** - SIM グループを展開します。
- **Property** - グループ情報をポップアップ画面で表示します。

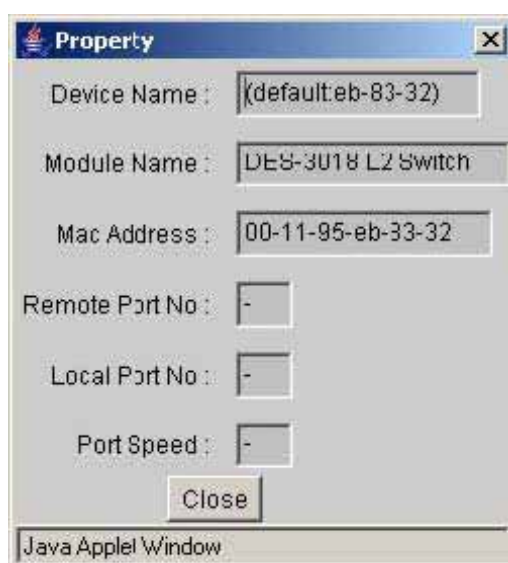



図 6- 41. Property 画面

Member Switch アイコン

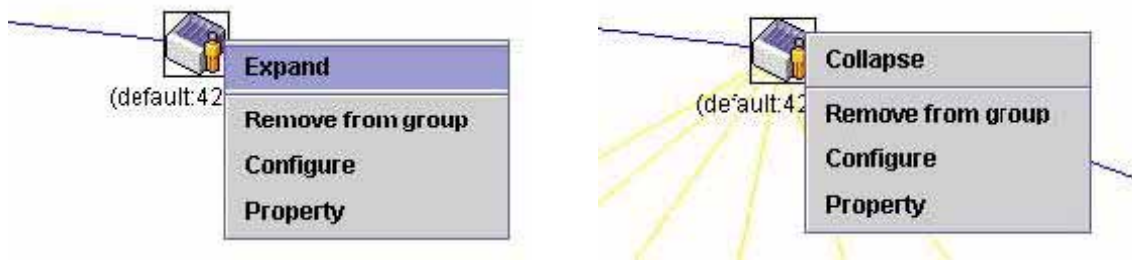



図 6- 42. Member アイコンを右クリックした例

以下のオプションが表示されます。:

- **Collapse** - シングルアイコンによって表示されるグループをまとめます。
- **Expand** - SIM グループを展開します。
- **Remove from group** - グループからメンバを削除します。
- **Configure** - スイッチの設定のためにWebブラウザを起動します。
- **Property** - グループ情報をポップアップ画面で表示します。

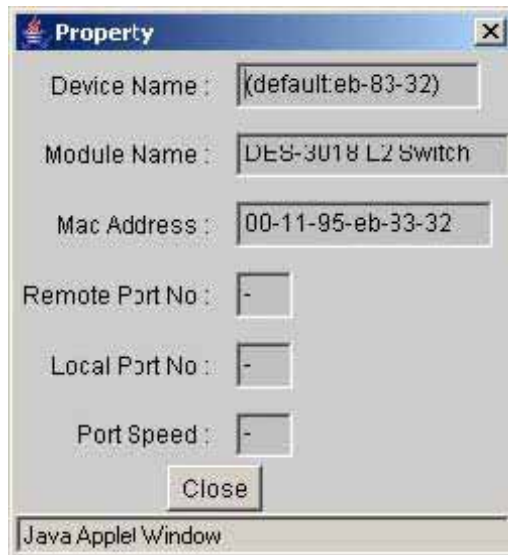



図 6- 43. Property 画面

Candidate Switch アイコン

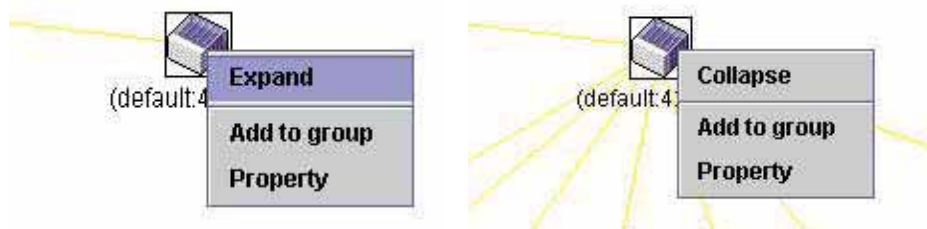



図 6- 44. Candidate アイコンを右クリックした例

以下のオプションが表示されます。:

- **Collapse** -シングルアイコンによって表示されるグループをまとめます。
- **Expand** - SIM グループを展開します。

- **Add to group** - SIMグループにCaSを追加します。このオプションをクリックし、SIMグループに追加する前に以下の画面でCaSから認証用パスワードを入力します。OKをクリックするか、キャンセルをクリックして本画面を終了します。

図 6- 45. Input password 画面

- **Property** - グループ情報をポップアップ画面で表示します。

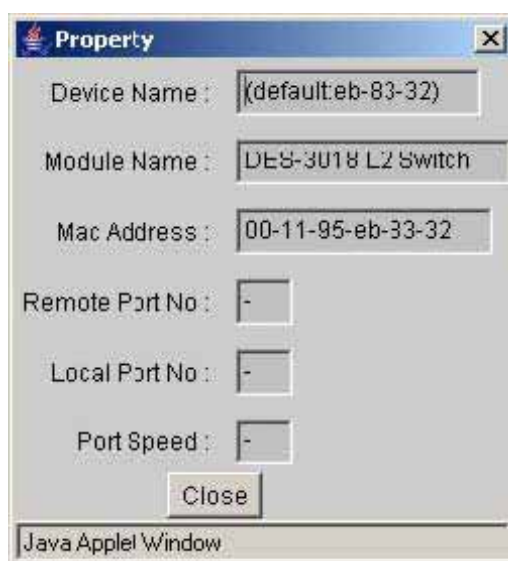



図6- 46. Device Property 画面

この画面には以下の情報があります:

パラメータ	説明
Device Name	ユーザに設定された SIM グループのデバイス名を表示します。デバイス名がない場合は名前として default が与えられ、識別のために MAC アドレスの終わり 6 文字が付加されます。
Module Name	マウスの右クリックで表示される製品名を表示します。
Mac Address	対応するスイッチの MAC アドレスを表示します。
Remote Port No	CS が接続している MS または CaS 上の物理ポート数を表示します。CS はこのフィールドにエントリを持ちません。
Local Port No	MS または CaS が接続している CS 上の物理ポート数を表示します。CS はこのフィールドにはエントリを持ちません。
Port Speed	CS と MS、または CaS 間のポートの接続速度を表示します。

Close をクリックし、**Property** 画面を終了します。

メニューバー

Single IP Management 画面にはデバイス設定のために以下のメニューバーがあります。

図 6- 47. トポロジービューのメニューバー

メニューバーには以下の 5 個のサブメニューがあります。

File

- **Print Setup** -印刷されるイメージを参照します。
- **Print Topology** - トポロジーマップを印刷します。
- **Preference** - ポーリング間隔、SIM起動時にオープンするビューなどの表示プロパティを設定します。

Group

- **Add to Group** - グループにCaSを追加します。このオプションをクリックし、SIMグループに追加する前に以下の画面でCaSから認証用パスワードを入力します。OKをクリックするか、キャンセルをクリックして本画面を終了します。

図 6- 48. Input password 画面

- **Remove from Group** - グループからMSを削除します。

Device

- **Configure** -指定デバイスのWebブラウザを開きます。

View

- **Refresh** -最新の状態にビューを更新します。
- **Topology** - トポロジービューを表示します。

Help

- **About** -現在のSIMバージョンを含むSIM情報を表示します。

確認: このファームウェアリリース時では、SIM のいくつかの機能は CLI(Command Line Interface)経由の設定になります。SIM およびその設定については ***Command Line Interface Reference Manual*** を参照ください。

ファームウェアアップグレード

以下の画面では CS からメンバスイッチのファームウェアをアップグレードします。**Administration > Single IP Setting > Firmware Upgrade** をクリックし、以下の画面を表示します。メンバスイッチはテーブル内にリストアップされ、**Port** (MS がある場所の CS 上のポート)、 **MAC Address**、**Model Name** および **Version** が表示されます。ファームウェアのダウンロードのために特定のスイッチを指定するには **Port** の先頭の下の対応するチェックボックスをクリックします。ファームウェアを更新するためにはファームウェアがある場所の **Server IP Address** を入力し、ファームウェアの **Path/Filename** を入力します。**Download** ボタンをクリックし、ファイル転送を開始します。

図 6- 49. Firmware Upgrade 画面

設定ファイルのバックアップ/リストア

以下の画面では CS から TFTP サーバを使用してメンバスイッチに設定ファイルのバックアップを行います。**Administration > Single IP Setting > Configuration Backup/Restore** をクリックし、以下の画面を表示します。メンバスイッチはテーブル内にリストアップされ **Port** (MS がある場所の CS 上のポート)、**MAC Address**、**Model Name** および **Version** が表示されます。設定ファイルのダウンロードのために特定のスイッチを指定するには **Port** の先頭にある対応するチェックボックスをクリックします。設定ファイルを更新するためにはファイルがある場所の **Server IP Address** を入力し、設定ファイルの **Path/Filename** を入力します。**Download** ボタンをクリックし、TFTP サーバからスイッチにファイル転送を開始します。**Upload** ボタンをクリックし、TFTP サーバに設定ファイルをバックアップします。

図 6- 50. Configuration File Backup/Restore 画面

フォワーディングとフィルタリング

ユニキャストフォワーディング

Administration > Forwarding & Filtering > Unicast Forwarding の順にメニューをクリックします。以下の **Setup Static Unicast Forwarding Table** 画面が表示されます。:

図 6- 51. Setup Static Unicast Forwarding Table と Static Unicast Forwarding Table 画面

エントリの追加や変更をするには以下のパラメータを設定し、**Add/Modify** ボタンをクリックします。

パラメータ	説明
VID	ユニキャスト MAC アドレスが存在する VLAN ID。
MAC Address	パケットが静的に転送される MAC アドレス。ユニキャスト MAC アドレスを指定します。
Allow to go Port	MAC アドレスが存在するポートの番号を選択します。

Add ボタンをクリックし、変更を適用します。現在のエントリが上図の下の **Static Unicast Forwarding Table** 内に表示されます。**Static Unicast Forwarding Table** 内のエントリを削除する場合は、対応する行の **Delete** 欄の ボタンをクリックします。

マルチキャストフォワーディング

以下の図と表はスイッチに **Multicast Forwarding** の設定を行うためのものです。**Administration > Forwarding&Filtering > Multicast Forwarding** とクリックし、以下の画面を表示します。

図 6- 52. Static Multicast Forwarding Settings と Current Multicast Forwarding Entries 画面

Static Multicast Forwarding Settings画面はスイッチに設定されたスタティックマルチキャスト転送テーブルのすべてのエントリを表示しています。**Add**ボタンをクリックし、以下の**Setup Static Multicast Forwarding Table**画面を表示します。

Setup Static Multicast Forwarding Table

VID	Multicast MAC Address
0	00-00-00-00-00-00

Port Settings	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
None	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿
Egress	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Apply

Show All Multicast Forwarding Entries

図 6- 53. Setup Static Multicast Forwarding Table

以下のパラメータを設定できます。

パラメータ	説明
VID	MAC アドレスに関連付けられた VLAN の VLAN ID です。
Multicast MAC Address	マルチキャストパケットの静的(スタティック)な送信元の MAC アドレスです。マルチキャスト MAC アドレスを指定します。
Port Settings	ポートがスタティックマルチキャストグループに所属するかどうかを選択します。 *None* -制限なしで動的にマルチキャストグループに参加できます。*None* のときポートはスタティックマルチキャストグループには所属しません。 *Egress* -ポートはマルチキャストグループに常に所属します。

Applyボタンをクリックし、変更を適用します。**Static Multicast Forwarding Table**からエントリを削除するには対応する行の**Delete**欄の ✕ ボタンをクリックします。Show All Multicast Forwarding Entriesリンクをクリックすると**Static Multicast Forwarding Settings**画面に戻ります。

マルチキャストフィルタリング

Administration > Fowarding&Filtering > Multicast Filtering Mode の順でメニューをクリックし、以下の画面を表示します。**Multicast Filtering Mode Setting** 画面を使用してマルチキャストパケットに対する2つのフィルタリングオプションから1つを選択します。:

- **forward unregistered groups** – すべてのマルチキャストパケットを転送します。(初期値)
- **filter unregistered groups** – 登録済みのマルチキャストグループにだけマルチキャストパケットを転送します。未登録のグループへのマルチキャストパケットはブロックされます。

図 6- 54. Multicast Filtering Mode 設定画面

Multicast Filtering Mode を設定して **Add** ボタンをクリックし、設定を適用します。

SMTP サービス

SMTP(Simple Mail Transfer Protocol)は、以下のコマンドを使用して入力した E-mail アドレスに基づくメール受信者にスイッチのイベントを送信するスイッチの機能です。スイッチは SMTP のクライアントとして設定され、一方サーバはスイッチからのメッセージを受信し、E-mail に適切な情報を記載し、スイッチに設定した受信者に送信するリモートデバイスです。これはスイッチ上に発生した問題イベントの記録を行い小ワークグループまたは配線用クローゼットの管理を簡素化し、緊急なスイッチのイベントの処理速度を向上させ、セキュリティを強化することができます。

スイッチは SMTP 機能内のクライアントとしての 4 つの重要な役割を果たします。:

- サーバとサーバの仮想ポートは、この機能が適切に動作するために正しく設定する必要があります。**SMTP Service Settings**画面でSMTPサーバアドレスとSMTPサーバポートフィールドを設定します。
- Mail受信者はスイッチに設定する必要があります。この情報はサーバに送信され、サーバは情報を処理後、受信者にスイッチ情報をE-mailで送信します。最大８人のE-mail受信者を**SMTP Service Settings**画面を使用してMail Receiver Addressを設定することでスイッチに設定できます。
- 管理者は設定した受信者に送信するメッセージから送信元メールアドレスを設定することができます。これにより管理者にスイッチの機能および問題についてより多くの情報を提供できます。個人のE-mailはSMTP Service Settings 画面のSelf Mail Address フィールドを使用して設定します。
- スイッチは受信者がSMTPサーバからスイッチに関するE-mailを受け取ることを最初に確認するためのテストメールの送信を設定できます。テストメールを設定するためには、SMTP機能は、はじめに**SMTP Service Settings**画面のSMTP Stateを設定して有効にし、**SMTP Service**画面でE-mailを送信します。SMTPに設定されたすべての受信者はSMTPサーバからサンプルのテストメッセージを受信します。

スイッチは以下のイベントが 1 つ以上発生すると受信者に E-mail を送信します。:

- スイッチがコールドスタートした場合。
- ポートがリンクダウン状態になった場合。
- ポートがリンクアップ状態になった場合。
- SNMP認証がスイッチによって拒否された場合。
- スイッチの設定エントリがNVRAMに保存された場合。
- ファームウェアのダウンロード中にTFTP上に異常が発生した場合。これにはTFTPサーバからの処理中(in-process)、不正ファイル(invalid-file)、不正動作(violation)、ファイルが見つからない(file-not-found)、完了(complete)、およびタイムアウト(time-out)メッセージが含まれます。
- スイッチにシステムリセットが発生した場合。

SMTP サーバからのスイッチイベントに関する E-mail 内の情報には以下の項目が含まれます。:

- 送信元のデバイス名とIPアドレス。
- スイッチから受信したメッセージの日付と時間と同様にメッセージを送信したSMTPサーバとクライアントを識別するタイムスタンプ。中継されたメッセージは各中継のタイム・スタンプを持っています。
- E-mailメッセージを送信している場合にスイッチに発生したイベント。
- 保存、ファームウェアのアップグレードのようにユーザによってイベントが処理された場合、タスクを完了したユーザのIPアドレス、MACアドレスおよびユーザ名が発生したイベントのシステムメッセージにともに送信されます。
- 一回以上同じイベントが発生すると、2回目のメールメッセージと続く各繰り返しのメッセージはメールメッセージのSubject行にシステムのエラーメッセージが記載されます。

Delivery Process 中に発生する詳しいイベントは以下のとおりです。

- 緊急メールは高いプライオリティを持ち、通常のメールがfutureキューにある間に受信者に直ちに送信されます。
- キュー内の未送信メールメッセージの最大数は30メッセージを超えることはできません。新しいメッセージはキューがいっぱいになると破棄されます。
- 初期メッセージがメール受信者に届かない場合、その後キュー内のその場所にメッセージを送信する別の試行があるまでwaitingキューにおかれます。
- メールの送信のための最大試行数は3です。メールメッセージの送信は最大試行数に到達するまで5分ごとに行われます。最大試行数に到達してもメッセージの送信が成功しない場合、メッセージは破棄されてメール受信者は受信することはできません。

スイッチがシャットダウンまたは再起動すると、waiting キューは消去されます。

SMTPサーバ設定

以下の画面のフィールドでスイッチに問題が発生した場合に設定した E-mail アドレスに従ってスイッチのログファイルを送信する SMTP サーバを設定します。**Administration > SMTP Service > SMTP Server Settings** の順でクリックし、以下の画面を表示します。

図 6- 55. SMTP Service Settings と Mail Receiver Address Table 画面

以下のパラメータが設定できます。

パラメータ	説明
SMTP State	プルダウンを使用してこのデバイスの SMTP サービスを有効または無効にします。
SMTP Server Address	リモートデバイスのSMTPサーバのIPアドレスを入力します。これはメールを送信するデバイスとなります。
SMTP Server Port	SMTP サーバに接続するスイッチの仮想ポート番号を入力します。一般的なポート番号は 25 です。1～65535 の間で指定することができます。
Self Mail Address	メールメッセージを送信する E-mail アドレスを入力します。このアドレスは受信者に送信された E-mail メッセージにある"from"のアドレスとなります。このスイッチには Self Mail Address を1つだけ設定することができます。この文字列には半角英数字 64 文字まで指定することができます。
Mail Receiver Address	スイッチ機能に関する E-mail メッセージを受信する受信者の E-mail アドレスのリストを入力します。8 個までの E-mail アドレスをスイッチに追加することができます。スイッチからアドレスを削除する場合は、Mail Receiver Address Table の Delete 欄で関連する ✕ をクリックします。

Apply ボタンをクリックし、変更を適用します。

SMTPサービス

以下の画面はスイッチに設定したすべてのメール受信者にテストメッセージを送信して SMTP サーバの設定および信頼性をテストするために使用します。**Administration > SMTP Service > SMTP Service** をクリックし、以下の画面を表示します。

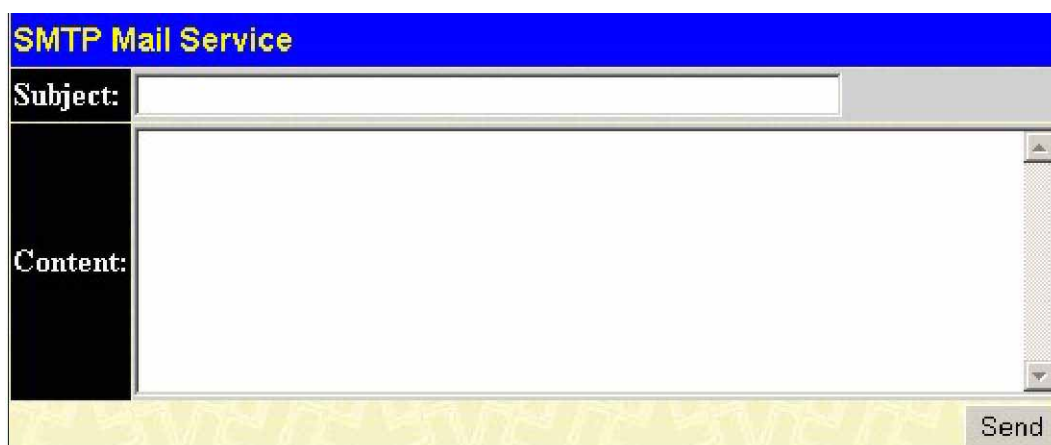



図 6- 56. SMTP Mail Service 画面

以下のパラメータを設定することができます。:

パラメータ	説明
Subject:	テスト E-mail の Subject を入力します。
Content:	テストE-mailの内容を入力します。

メッセージの準備ができたら **Send** ボタンをクリックしてスイッチに設定したすべての受信者にこのメールを送信します。

セクション 7

レイヤ2機能

VLAN

VLAN について

VLAN(Virtual Local Area Network)はスイッチにある任意のポートを論理的にグループ化したネットワーク形態です。VLAN により任意の LAN セグメントをユーザによって管理されるグループ化した一つの LAN として結合することができます。また、VLAN はネットワークを異なるブロードキャストドメインに論理的に分割するので、パケットは同一の VLAN に所属したポート間のみで送信されます。必ずしも必要ではないが、通常、ひとつの VLAN はそれぞれ特定のサブネットに対応しています。

VLAN は帯域幅を確保することによって性能を高めたり、トラフィックを特定のドメインに制限することによって、セキュリティを向上させることができます。

VLAN は物理的な位置の代わりに論理によって分類されたエンドノードの集合です。それらが物理的にネットワークのどこにあるかにかかわらず、頻繁に互いに通信するエンドノードが同じ VLAN に割り当てられます。VLAN はブロードキャストパケットをブロードキャストが発信された VLAN のメンバのみに送るので、論理的にはブロードキャストドメインと同一視することができます。

本スイッチでのVLANの注意点

個々のエンドノードを特定したり、それらのノードがなんらかの VLAN のメンバだった場合もネットワークデバイスにより VLAN 間のルーティングが設定されていない限り、パケットは VLAN に所属していないポートに送信されることはありません。

本スイッチは IEEE802.1Q VLAN とポートベースの VLAN をサポートしています。タグに対応しないデバイスとの互換性を維持するために、ポートアンタギング機能によりパケットヘッダから 802.1Q タグを取り除くことができます。

本スイッチは初期状態ではすべてのポートが VLAN「default」に所属しています。

「default」VLAN の VID は「1」になっています。

ポートベース VLAN では 1 つのポートは複数の VLAN に所属することができます。

IEEE 802.1Q VLAN

以下は関連する項目です。

タグ付け - パケットのヘッダに 802.1Q VLAN 情報を入れること。

タグ取り - パケットヘッダから 802.1Q VLAN 情報を削除すること。

イングレスポート - パケットを受信するポート。このポートでは受信パケットにタグが含まれているかを確認して処理します。

イーグレスポート - パケットを送信するポート。このポートではスイッチ、またはネットワークに送信するときにタグ VLAN 情報を付与するかどうかを決定します。

本スイッチは(タグ付き)IEEE 802.1Q VLAN をサポートしています。ネットワークのすべてのスイッチが IEEE 802.1Q 対応であるならば、タグ付けをすることにより全体のネットワークに 802.1 Q VLAN を使用することができます。

VLAN はブロードキャストドメインのサイズを減少させるためにネットワークを分割できます。VLAN を使用することによりネットワークを細かく分け、個々のブロードキャストドメインのサイズを小さくすることができます。すなわち、VLAN 上のすべてのパケット

(任意のソースからのユニキャスト、マルチキャスト、そしてブロードキャストパケットすべて)は IEEE 802.1Q に対応したスイッチ経由でその VLAN に所属する端末にのみ送信されます。

また、VLAN はネットワークにセキュリティ機能を加えることができます。IEEE 802.1Q VLAN はパケットを VLAN のメンバである端末にのみ送信します。

すべてのポートはタグ付き/タグなしに設定できます。タグなしの場合、IEEE 802.1Q VLAN は、パケットヘッダで VLAN タグを認識しない旧式のスイッチでも動作します。タグを付けることにより複数の 802.1Q 対応スイッチを物理的に接続し、その接続上で VLAN を構成し、すべてのポートにおいてスパニングツリーを有効にして正常動作させることができます。

IEEE 802.1Q 標準では受信ポートが VLAN に所属している場合、タグなしパケットは転送されません。

- フィルタリングによりパケットを VLAN に割り当てます。
- 全体で 1 つのスパニングツリーが構成されていると仮定します。
- 1 レベルのタグ付けによるタグ付けを行います。
- 802.1Q VLAN のパケット転送
- パケットの転送は以下の 3 つの種類のルールに基づいて決定されます。:

  イングレスルール - 受け取ったパケットがどの VLAN に所属するかの分類に関するルール。

  ポート間のフォワーディングルール - 転送するかしないかを決定します。

  イーグレスルール - パケットが送信されるときにタグ付きかタグなしかを決定します。

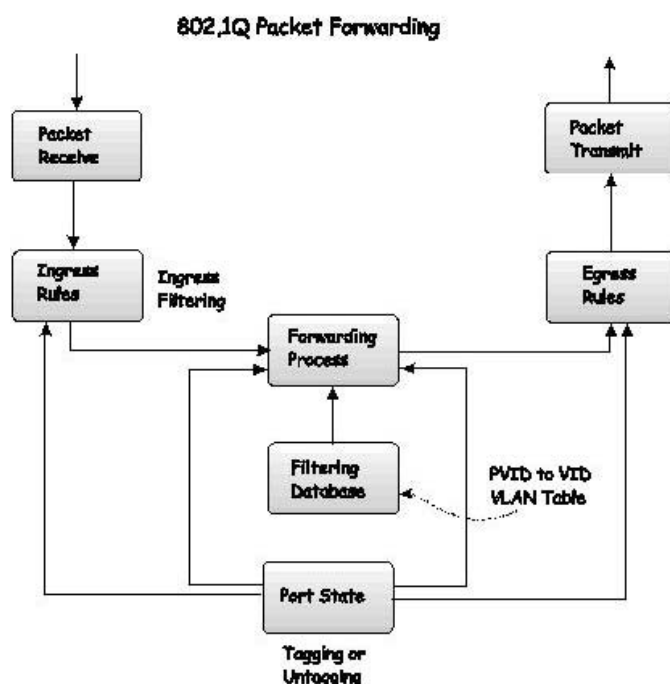



図 7- 1. IEEE 802.1Q のパケット転送

802.1Q VLAN タグ

次の図は 802.1Q VLAN のタグについて表示しています。ソース MAC アドレスの後に 4 オクテットのフィールドが挿入されています。それらが存在する場合、EtherType フィールドの値は 0×8100 になります。つまり、パケットの EtherType フィールドが 0×8100 と等しいときに、パケットには IEEE 802.1Q/802.1p タグが含まれています。タグは以下の 2 オクテットに含まれていてユーザプライオリティの 3 ビット、CFI(Canonical Format Identifier: トークンリングパケットをカプセル化してイーサネットバックボーンをはさんで転送するためのもの)の 1 ビット、および VID(VLAN ID)の 12 ビットから成ります。ユーザプライオリティの 3 ビットは 802.1p によって使用されます。VID は VLAN を識別するためのもので 802.1Q 標準によって使用されます。VID は長さ 12 ビットなので 4094 のユニークな VLAN を構成することができます。

タグはパケットヘッダに埋め込まれ、パケット全体は 4 オクテット長くなります。そして、元々のパケットに含まれていた情報のすべてが保持されます。

IEEE 802.1Q Tag

Octets
0 1 2 3 4
Destination Address (6 octets)
Source Address (6 octets)
EtherType = 0x8100 | Tag Control Information
MAC Length/Type | Begining of Data
Cyclic Redundancy Check (4 octets)
User Priority | CFI | VLAN ID (VID) (12 bits)
3 bits | 1 bit | 12 bits

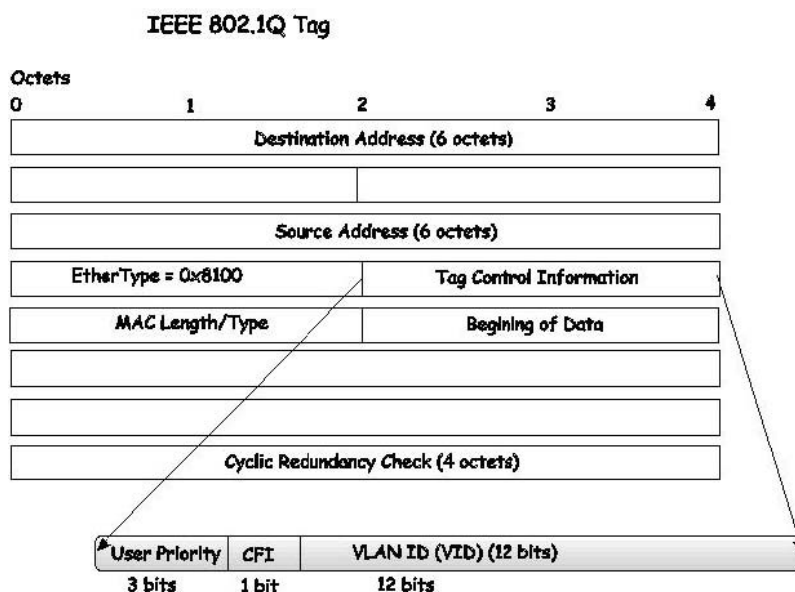



図 7- 2. IEEE 802.1Q タグ

EtherType と VLAN ID はソース MAC アドレスと元の EtherType/Length か Logical Link Control の間に挿入されます。パケットは元のものよりも少し長くなるので、CRC は再計算されます。

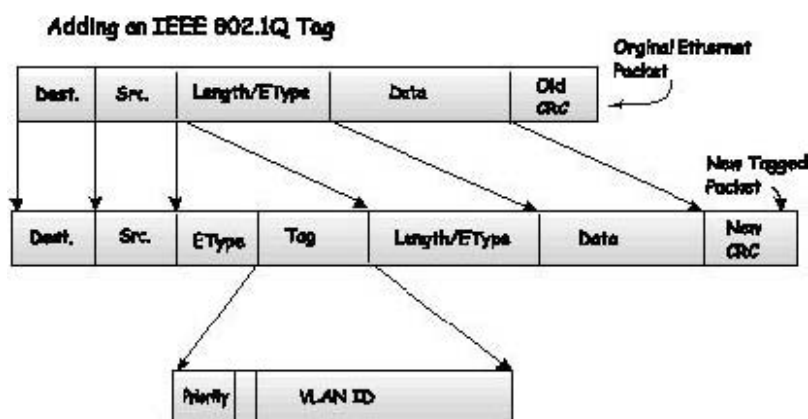



図 7- 3. IEEE 802.1Q タグの追加

タグ付きとタグなし

802.1Q 対応のスイッチのすべてのポートは、タグ付きかタグなしに設定できます。

タグ付きのポートは受信、送信するすべてのパケットのヘッダに、VID、プライオリティ、そしてそのほかの VLAN 情報を埋め込みます。パケットがすでにタグ付けされていたなら、VLAN 情報を完全に保つためにポートはパケットを変更しません。ネットワーク上の他の 802.1Q 対応デバイスも、タグの VLAN 情報を使用してパケットの転送を決定します。

タグなしのポートは、受信、送信するすべてのパケットから 802.1Q タグを削除します。パケットに 802.1Q VLAN タグがなければ、ポートはパケットを変更しません。つまり、タグなしのポートが受信して、転送したすべてのパケットは 802.1Q VLAN 情報をまったく持ちません。PVID はスイッチの内部で使用されるだけです。タグなしはパケットを 802.1Q 対応のデバイスから、非対応のデバイスにパケットを送信するのに使用します。

イングレス・フィルタリング

スイッチがパケットを受信し、VLAN を決定するポートをイングレスポートと呼びます。ポートでイングレス・フィルタリングを可能にすると、スイッチはパケットヘッダに VLAN 情報が付加されていればそれを調べ、パケットを転送するかどうかを決定します。

パケットが VLAN 情報にタグ付けされている場合、イングレスポートは最初にイングレスポート自体がタグ付けをされた VLAN のメンバであるかどうか判定します。メンバでない場合、パケットを破棄します。イングレスポートが 802.1Q VLAN のメンバであれば、次に送信先ポートが 802.1Q VLAN のメンバであるかどうか判定します。メンバでない場合、パケットを破棄します。送信先ポートが 802.1Q VLAN のメンバであれば、パケットを転送し、送信先ポートはそれを接続されたネットワークセグメントに伝えます 。

パケットが VLAN 情報にタグ付けされていない場合、イングレスポートがタグ付けポートであれば、そのポートの PVID を VID としてパケットにタグ付けします。そして、送信先ポートがイングレスポートとして同じ VID を持った VLAN のメンバであるかどうか判定します。メンバでない場合、パケットは破棄されます。VID が同じ場合、パケットを転送し、送信先ポートは接続されたネットワークセグメントに伝えます。

これがイングレス・フィルタリングと呼ばれる機能で、受信先がイングレスポートと同じ VLAN にない場合にパケットを破棄して帯域幅を節約します。これにより送信先ポートにパケットが送られてから破棄されるという処理を省くことができます。

デフォルトVLAN

スイッチでは、最初に「default」という名で VID が 1 の VLAN が構成されています。出荷時設定ではスイッチ上のすべてのポートが「default」に割り当てられています。新しい VLAN がポートベースモードで構成されるとき、その VLAN に所属するポートは「default」から削除されます。

パケットは VLAN 間をまたぐことはできません。ある VLAN に所属するポートが他の VLAN に接続したい場合、外部のルータを経由しなくてはなりません。

確認: VLAN が設定されていない場合、すべてのパケットはすべてのポートに転送されます。未知の送信元アドレスを持つパケットもすべてのポートに送信されてしまいます。さらに、ブロードキャストパケット、そしてマルチキャストパケットもすべてのポートに送信されてしまいます。

例を以下に示します。

表 7- 1. VLAN の例 - ポートの割り当て

VLAN 名	VID	スイッチポート
System (default)	1	5, 6, 7, 8, 21, 22, 23, 24
Engineering	2	9, 10, 11, 12
Marketing	3	13, 14, 15, 16
Finance	4	17, 18, 19, 20
Sales	5	1, 2, 3, 4

VLAN のセグメンテーション

VLAN2 に所属するポート 1 に接続したデバイスから送信されたパケットを例に挙げます。もし、送信先が通常の転送テーブル検索で見つかるような別のポート(ポート 10 とします)にある場合、スイッチはそのポート 10 が VLAN2 に所属し、VLAN2 のパケットを受信できるかを調べます。もしポート 10 が VLAN2 に所属していない場合、パケットは破棄され、送信先には送られることはありません。ポート 10 が VLAN2 に所属しているならば、パケットは転送されます。これらの各 VLAN に基づく選択性のある転送が、VLAN によるネットワークの分割です。重要なのはポート 1 は VLAN2 のみに送信するということです。

VLAN と トランクグループ

ひとつのトランクグループのメンバは同じVLANに所属します。つまり、あるトランクグループに所属するメンバに対するVLANの設定のすべては他のメンバのポートにも適用されます。

スタティックVLAN エントリ

L2 Features > Static VLAN Entry をクリックし、以下の画面を表示します。

図 7- 4. 802.1Q Static VLANs 画面

Current 802.1Q Static VLAN Entries 画面で、すでに設定されている VLAN ID と VLAN 名を表示します。既存の 802.1Q VLAN を削除するには対応する行の Delete 欄の ボタンをクリックします。

新しい、802.1Q VLAN を作成するには **Add** ボタンをクリックし、以下の **802.1Q Static VLANs** 画面を表示します。ポート、重複しない VID、VLAN 名を設定します。画面内のパラメータについては以下の表を参照してください。

図 7- 5. 802.1Q Static VLANs 画面 – 追加

Current 802.1Q Static VLAN Entries画面に戻るためには、Show All Static VLAN Entriesリンクをクリックします。既存の802.1Q VLANを変更するには変更したいVLANに対応した行の**Modify**ボタンをクリックします。ポート、重複しないVID、VLAN名を設定するための新しい画面が表示されます。画面内のパラメータについては以下の表を参照してください。

図 7- 6. 802.1Q Static VLANs 画面- 修正

以下のパラメータは**802.1Q Static VLANs**の**Add** および **Modify** 画面で設定できるものです。

パラメータ	説明
VID (VLAN ID)	Add 画面では VLAN ID を入力します。Modify 画面では VLAN ID を表示します。VLAN は VID または VLAN 名を識別します。
VLAN Name	Add 画面では VLAN 名を入力します。Modify 画面では VLAN 名を編集します。
Port Settings	VLAN に所属するポートを指定します。
Tag	ポートを 802.1Q タグ付きか 802.1Q タグなしかに指定します。チェックするとタグ付きになります。
None	ポートを VLAN メンバから除外します。
Egress	ポートを VLAN のスタティックメンバとします。イーグレスメンバポートは VLAN 向けにトラフィックを送信するポートです。これらのポートはタグ付きにも、タグなしにも設定できます。

Apply ボタンをクリックし、設定を有効にします。**802.1Q Static VLANs** 画面に戻るためには Show All Static VLAN Entries リンクをクリックします。

リンクアグリゲーション

ポートトランクグループについて

ポートトランクグループは複数のポートを結合して、単一の高帯域データパイプラインを作ります。本シリーズは各グループに2から8のポートを結合でき、最大32のポートトランクグループをサポートし、最高8000Mbpsの転送速度で通信が可能です。

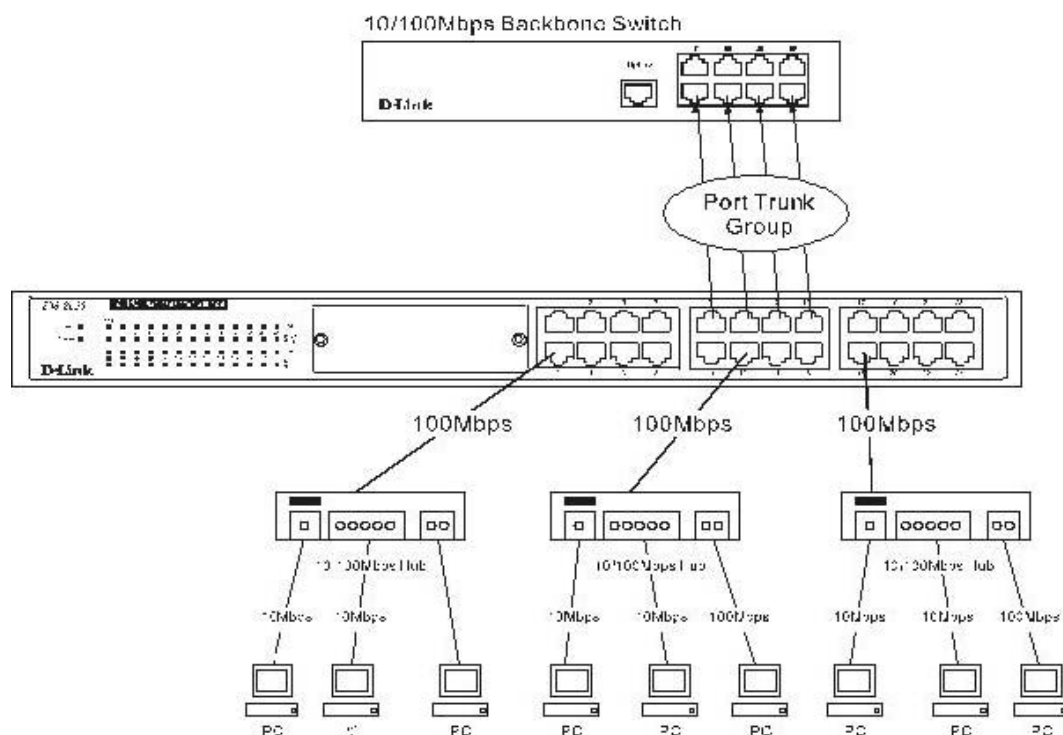



図 7- 7. ポートトランクグループの例

スイッチはトランクグループのすべてのポートを単一のポートとして扱います。特定のホスト(送信先アドレス)に送られるデータは常にトランクグループの同一のポートに送られます。こうしてデータ・ストリームのパケットは送られた順に到着します。

確認: トランクグループ中のいずれかのポートが切断した場合、パケットはトランクグループの残りのポートを使用して送信されれます。

リンク・アグリゲーションはいくつかのポートをひとつにまとめて単一のリンクとして動作します。帯域は単一のリンクによる帯域の倍数になります。

リンク・アグリゲーションは一般的に、サーバやネットワークのバックボーンへの接続のように帯域の確保と冗長性が必要なネットワークで使用します。

2 から 8 個のリンク(ポート)で構成できる最大 3 個のリンク・アグリゲーショングループを作ることができます。トランクグループのポートのすべては同じ VLAN に所属し、STP ステータス、スタティックマルチキャスト、トラフィックコントロール、トラフィックセグメンテーション、および 802.1p デフォルトプライオリティ設定は同じである必要があります。トランクグループでポートロック、ポートミラーリング、および 802.1X を有効にすることはできません。さらに、集められたポートはすべて同じ速度で、全二重である必要があります。

グループのマスターポートはユーザが設定し、マスターポートに適用する VLAN 設定を含むすべての設定オプションはリンク・アグリゲーショングループに適用されます。

ロードバランス(負荷分散)機能は自動的にグループの各ポートに適用され、トランキングで通信中にあるポートのリンク切れが起こった場合、残ったポートで通信を行います。

スパニング・ツリープロトコル(STP)はスイッチレベルでリンク・アグリゲーショングループを単一のリンクとして扱います。ポートレベルでは、STP はマスターポートの設定を使用しポートコストの計算とリンク・アグリゲーショングループの状態を決定します。2 つの冗長なリンク・アグリゲーショングループがスイッチ上で構成されると、冗長なリンクがあるポート単体もブロックするように STP は片方のグループを丸ごとブロックします。

ポートトランキングを設定するには **L2 Features > Trunking > Link Aggregation** の順でクリックし、以下の画面を表示します。

図7- 8. Port Trunking Group 画面

ポートトランクグループを構成するには **Add** ボタンをクリックして新しいトランクグループを加え、以下の **Port Trunking Configuration** 画面でトランクグループの設定をします。ポートトランクグループの設定を変更するためには変更したいエントリの Group ID のリンクをクリックします。ポートトランクグループを削除するには **Current Trunking Group Entries** 画面で対応する行の **Delete** 欄の ボタンをクリックします。

図 7- 9. Port Trunking Configuration 画面 – 追加

IGMP Snooping

Internet Group Management Protocol (IGMP) snooping を使用すると、ネットワークステーション、デバイスと IGMP ホストの間の IGMP クエリとレポートを認識することができます。IGMP snooping を有効にすると、スイッチを通過する IGMP メッセージを元に特定のデバイスに対してポートの開閉を行うことができます。

IGMP Snoopingを使用するためには、はじめにスイッチ全体の設定でIGMP Snoopingを有効にします(**Advanced Settings**参照)。次に**L2 Features > IGMP Snooping** をクリックしてそれぞれのVLANに対して設定を行います。IGMP snoopingを有効にすると、スイッチはデバイスからIGMPホストに対して送られてきた、もしくはその逆向きのIGMPメッセージに基づき特定のマルチキャストグループメンバに対してポートを開閉します。

スイッチは IGMP メッセージをモニターし、パケット転送を継続するリクエストを行うホストがなくなると、マルチキャストパケットの転送を中止します。

IGMP Snooping Settings 画面を使用して **IGMP Snooping** 設定を参照します。設定を変更するためには変更したい VLAN ID 行の **Modify** ボタンをクリックします。

IGMP Snooping Settings

VLAN ID	VLAN Name	State	Querier State	Modify
1	default	Disabled	Disabled	Modify

図 7- 10. IGMP Snooping Settings 画面

Modify ボタンをクリックし、以下の **IGMP Snooping Settings** 画面を表示します。

IGMP Snooping Settings

VLAN ID	1
VLAN Name	default
Query Interval (1-65535)	125
Max Response Time (1-25)	10
Robustness Value (1-255)	2
Last Member Query Interval (1-25)	1
Host Timeout (1-16711450)	260
Router Timeout (1-16711450)	260
Leave Timer (1-16711450)	2
Querier State	Disabled
Querier Router Behavior	Non-Querier
State	Disabled
Multicast fast leave	Disabled

Apply

Show All IGMP Group Entries

図 7- 11. IGMP Snooping Settings 画面 – 変更

以下のパラメータを確認、変更できます。

パラメータ	説明
VLAN ID	IGMP Snooping の設定を変更する VLAN の VLAN ID。VLAN Name と同期しています。
VLAN Name	IGMP Snooping の設定を変更する VLAN の VLAN 名。VLAN ID と同期しています。
Query Interval(1-65535)	IGMP クエリを送信する間隔を秒単位で設定します。*1* から *65535* までで設定でき、初期値は *125* です。
Max Response Time (1-25)	IGMP レスポンスレポートを送信するまでの最大許容時間を秒単位で設定します。*1* から *25* までで設定でき、初期値は *10* です。
Robustness Variable **(1-255)**	予想されるパケットの損失に応じてこの変数を調整します。VLAN におけるパケットの損失が高いと予想できる場合、Robustness Variable はパケット損失の増加をカバーするために増やします。*1* から *255* までで設定でき、初期値は *2* です。
Last Member Query Interval **(1-25)**	各グループにおける、リーブグループメッセージに対するレスポンスの送信も含むクエリメッセージの最大の間隔を秒単位で設定します。初期値は *1* です。
Host Timeout **(1-16711450)**	ホストからのメンバシップレポートなしでもそのホストをマルチキャストグループのメンバとみなす最大の時間を秒単位で設定します。初期値は *260* です。
Router Timeout **(1-16711450)**	メンバシップレポートなしで経路を転送テーブルに保持する最大の時間を秒単位で設定します。初期値は *260* です。
Leave Timer **(1-16711450)**	スイッチがグループメンバシップクエリを発行してから、ホストからリーブグループメッセージを受け取るまでの最大の時間を秒単位で設定します。**Leave Timer** で設定された時間が来るまでにメンバシップクエリにレスポンスがないなら、ホストに対するマルチキャスト転送は行われなくなります。
Querier State	*Enabled* を選ぶと IGMP クエリパケットを転送し、*Disabled* では転送しません。初期値は *Disabled* です。
Querier Router Behavior	このフィールドは参照用でルータがクエリパケットを送信する動作について表示します。*Querier* はルータが IGMP クエリパケットを送信していることを示します。*Non-Querier* は IGMP クエリパケットを送信していないことを示します。このフィールドは **Querier State** と **State** フィールドが Enabled(有効)である場合に Querier を読み取ります。
State	IGMP Snooping の有効/無効を設定します。初期値は *Disabled* です。
Multicast fast leave	このパラメータにより *Fast Leave* 機能が有効になります。Enabled(有効)にすると、この機能はスイッチが IGMP Leave Report パケットを受信する場合にマルチキャストグループのメンバをただちに(Last Member Query Timer の実行なしで)グループから離脱させることができます。初期値は(無効)です。

Applyボタンをクリックし、変更を適用します。Show All IGMP Snooping Entries リンクをクリックすると**IGMP Snooping Group Entries**画面に戻ります。

確認: Fast Leave 機能はマルチキャストグループから離脱したい IGMPv2 ユーザのための機能であり、各ポートに接続しているホストを1つだけ持つ VLAN で実行するのに最適です。ホストグループの1つのホストが Fast Leave 機能を使用する場合、グループの他のホストの意図しない離脱を引き起こす可能性があります。

スタティックルータポート設定

スタティックルータポートはマルチキャストルータを接続するためのポートです。一般にこのようなルータは WAN やインターネットに接続しています。ルータポートを設定することにより、ルータから送信されたマルチキャストパケットをネットワーク全体に送信したり、ネットワークから送信されたマルチキャストメッセージ(IGMP)をルータが受信することが可能になります。

ルータポートは以下の機能を持ちます。

- すべてのIGMPレポートパケットはルータポートに転送されます。
- ルータポートからのIGMPクエリはすべてのポートに送られます。

UDP マルチキャストパケットはすべてルータポートに転送されます。UDP マルチキャストパケットがすべてルータポートに転送されないと、UDP データストリームを受け取ることができないレイヤ 3 スイッチのルータポートに接続されたマルチキャストルータは IGMP レポートの送信および IGMP snooping は行いません。

ルータポートは IGMP クエリパケット、RIPv2 マルチキャスト、DVMRP マルチキャストそして PIM-DM マルチキャストパケットをポートで受信したときに動的に構成されます。

L2 Features > IGMP Snooping > Static Router Ports Settings をクリックし、以下の **Static Router Port Settings** 画面を表示します。

Total Entries:2

Static Router Port Settings

VLAN ID	VLAN Name	Modify
1	default	Modify
2	Darren	Modify

図 7- 12. Static Router Ports Settings 画面

上記の **Static Router Ports Settings** 画面は静的なルータポートテーブルに現在のエントリをすべて表示します。エントリを変更するには **Modify** ボタンをクリックし、以下の **Static Router Ports Settings** 画面を表示します。

図 7- 13. Static Router Ports Settings – 編集画面

以下のパラメータを設定できます。

パラメータ	説明
VID (VLAN ID)	マルチキャストルータを接続する VLAN ID です。VLAN Name と同期しています。
VLAN Name	マルチキャストルータを接続する VLAN 名です。
Member Ports	マルチキャストルータを接続するポートです。

Apply ボタンをクリックし、設定を適用します。Show All Static Router Ports Entries リンクをクリックすると **Current Static Ports Settings** のエントリ画面に戻ります。

スパニングツリー

本スイッチは802.1d STPおよび802.1w Rapid STPの2つのバージョンのスパニングツリープロトコルをサポートしています。802.1d STPはほとんどのネットワークのプロにとってよく知られた機能です。ここではD-Linkマネージメントイーサネットスイッチがサポートする802.1d STPおよび802.1w Rapid STPの設定方法について簡単に説明します。

802.1w Rapid Spanning Tree

本スイッチは 802.1d STP および 802.1w Rapid STP の 2 つのスパニングツリープロトコルをサポートしています。IEEE 802.1w で定義されている Rapid Spanning Tree Protocol (RSTP)、そして互換性のある IEEE 802.1d STP です。RSTP は IEEE 802.1d サポートの古いデバイスでも使用できますが、RSTP のメリットは失われます。

IEEE 802.1w Rapid Spanning Treeプロトコル(RSTP)は802.1d STP規格から発展しました。RSTPは最近の革新的なスイッチ機能(特にイーサネットスイッチで多く取り扱われるL3機能)を妨害するSTPの限界を克服するために開発されました。基本機能と使用する用語の多くはSTPと同じです。また、STPのために構成した設定の大部分はRSTPに使用されます。本セクションではいくつかの新しいSpanning Tree概念を紹介して2つのプロトコルの主な違いを例証します。

Port Transition States

2 つのプロトコルの本質的な相違は転送ステータスにおけるポートの変化と、転送と非転送のトポロジーにおけるポートの役割に関連する変化です。RSTP は 802.1d で使われる Disabled、Blocking、Listening、そしてさらに Discarding というトランジションステータスがあります。いずれの場合もポートはパケットを転送しません。STP ポートトランジションステータスの Disabled、Blocking、Listening、そして、RSTP の Discarding には機能的な違いはありません。ポートはネットワークトポロジーの観点からは無効です。以下の表 6-2 は 2 つのプロトコルのポートステータストランジションがどのように異なるかを比べています。

2つのプロトコルはすべて、同じ方法で安定したトポロジーを算出します。すべてのセグメントはルートブリッジに対して1つの経路しか持ちません。すべてのブリッジはBPDUパケットを監視します。しかし、BPDUパケットはHelloパケットよりも頻繁に送信されます。BPDUパケットはBPDUパケットが受信されなくても送信されます。そのため、ブリッジ間のそれぞれのリンクはリンクステータスに依存します。これは早期のリンク障害の検出につながり、トポロジーの調整も早くなります。802.1dの欠点は隣接しているブリッジからすぐにフィードバックが来ないことです。

表 6- 2. ポートステータスの比較

802.1w RSTP	802.1d STP	Forwarding	Learning
Disabled	Disabled	No	No
Discarding	Blocking	No	No
Discarding	Listening	No	No
Learning	Learning	No	Yes
Forwarding	Forwarding	Yes	Yes

RSTP はタイマーの設定にたよらず、RSTP に準拠したブリッジ同士のリンクによって、転送ステータスの変更をすばやく行うことができます。ポートは転送ステータスを変更する前にトポロジーが安定するのを待つ必要はありません。高速な変更を行うためにプロトコルはエッジポートと Point to Point(P2P)ポートという 2 つの要素を導入しています。

エッジポート

エッジポートはループが起こりえない位置に直接接続したポートに対する設定です。その例としてはポートにワークステーションが直接 1 つだけ接続している状態です。エッジポートとして設定されると、外部のステータスを監視したり、学習したりせずに、すぐに転送ステータスに変更します。BPDU パケットを受信するとエッジポートはステータスを削除し、すぐに普通のスパニングツリーポートになります。

P2P ポート

P2P ポートも同様に高速な変更が可能です。P2P ポートは他のブリッジに接続して使用されます。RSTP では全二重で動作するすべてのポートは P2P ポートとみなされ、手動で設定することなくその設定は上書きされます。P2P ポートも同様に高速な変更が可能です。P2P ポートは他のブリッジに接続して使用されます。

802.1dと802.1wの互換性

RSTP は旧式のデバイスと相互に使用することができ、必要であれば 802.1d フォーマットの BPDU パケットを自動的に生成して使用することができます。しかし、802.1d STP を使用するセグメントでは RSTP の高速な変更と高速なトポロジー変化検出のメリットを受けることはできません。また、これらのプロトコルは、セグメントに存在する旧式のデバイスを RSTP を使用できるデバイスに置き換えるために使用する変数を用意しています。

Spanning Tree Protocol (STP)の設定には 2 段階あります。

1. スイッチのレベルで全体的な設定を行う。
2. ポートレベルでユーザが定義するポートグループの基本設定を行う。

STPループバック検出

他のスイッチに接続した場合、STP はポートに送信するパケットにとって重要な設定であり、ご使用のスイッチのスループットを大きく向上させることができます。今のところ、この機能は本スイッチに接続しているアンマネージドスイッチからループバックされる BPDU パケットのように本スイッチに時々ループバックする STP BPDU パケットには正常に動作しません。本スイッチはスループットを持続するために STP ループバック防御機能をサポートしています。

STP ループバック検出機能が有効である場合、本スイッチはスイッチ間に発生するループバックから防御されます。一度 BPDU パケットがスイッチに戻ると、この機能は異常が発生していることを検出し、受信ポートをエラーにより無効であるという状態にします。さらにメッセージはスイッチの Syslog 内に保存され、そこには"BPDU Loop Back on Port #"のように定義されます。

ループバックタイマーの設定

ループバックタイマーはこの問題を解決する次の段階への鍵となる役割を果たします。タイマーには 0 ではない値を指定し、Auto-Recovery メカニズムを有効にします。このタイマーが終了するとスイッチは同じポートに BPDU パケットが戻ってきていることを再び検索します。パケットを受信していなければスイッチはポートを Discarding State に戻します。別の BPDU パケットを受信すると、ポートは防御ステータスのままとなり、タイマーは指定値にリセットされて再度開始されます。

この機能を使用しない場合は LoopBack Recovery time を 0 に設定します。この場合、BPUDU パケットはスイッチに戻り、ポートは防御状態になり、メッセージがスイッチの Syslog に送信されます。ポートを回復するためには、管理者は問題の発生したポートを無効にして、再度有効にする必要があります。これは LoopBack Recover Time が 0 に設定されている場合にポートを回復できる唯一の方法です。

ループバック検出機能の規則と制限

STP (STP と RSTP)のすべてのバージョンがこの機能を有効にすることができます。

グローバルに設定される可能性があります。(STP Global Bridge Settings)

本スイッチの隣接スイッチも BPDU パケットを転送できる必要があります。この要求仕様に合わせないスイッチは本スイッチ上の当該ポートに対してこの機能が無効となります。

この機能の初期値は無効です。

LoopBack タイマーの初期値は 60 秒です。

この設定はインタフェースが STP を有効にしている場合にだけ使用できます。

LoopBack 検出機能は指定ポートへの BPDU ループを防御するだけです。エッジポートに接続しているユーザ側に発生しているループ状態は検出できますが、別のスイッチの決められた STP のルートポートのループバックを検出することはできません

STP ブリッジグローバル設定

Layer 2 Features > Spanning Tree > STP Bridge Global Settings の順にクリックし、以下の画面を表示します。

Switch Spanning Tree Settings	
Spanning Tree Protocol	Disabled
Bridge Max Age (6-40 Sec)	20
Bridge Hello Time (1-10 Sec)	2
Bridge Forward Delay (4-30 Sec)	15
Bridge Priority (0-61440)	32768
Default Path Cost	802.1T
STP Version	RSTP
TX Hold Count(1-10)	3
Forwarding BPDU	Enabled
LBD	Disabled
LBD Recover Time(0:Disable)	60
	Apply
Designated Root Bridge	--
Root Priority	--
Cost to Root	--
Root Port	--
Time Topology Change(Sec)	--
Topology Changes Count	--
Protocol Specification	--
Max Age	--
Hello Time	--
Forward Delay	--
Hold Time	--

Note: 2(Forward Delay-1) >= Max Age,*
Max Age >= 2(Hello Time +1)*

図 7- 14. Switch Spanning Tree Settings

確認: Hello Time は Max Age より長くはできません。長くするとエラーになります。パラメータを設定する場合には以下の条件を参照してください。

Max. Age <= 2 x (Forward Delay – 1 秒)

Max. Age <= 2 x (Hello Time + 1 秒)

以下のSTPのパラメータを設定できます。

パラメータ	説明
Spanning Tree Protocol	プルダウンメニューを使用し、STP の有効/無効を設定します。初期値は *Disabled*(無効)です。
Bridge Max Age (6 - 40 Sec)	**Max Age** は古い情報がネットワーク上の冗長経路が循環しているものではないことを保証し、新しい情報が伝播することを防ぐためのものです。ルートブリッジにより設定され、ブリッジ接続した LAN 上にある他のデバイスと矛盾しないスパニングツリー設定を行うのに役立ちます。この値以上の時間がたってもルートブリッジからの BPDU を受信していない場合、スイッチは自身の BPDU を他のルートブリッジになることができるすべてのスイッチへの送信を開始します。もっとも低い Bridge Identifier を持つスイッチがルートブリッジになります。*6* から *40* 秒で設定でき、初期値は *20* 秒です。
Bridge Hello Time (1 - 10 Sec)	**Hello Time** は *1* から *10* 秒まで設定できます。ルートブリッジが自分自身がルートブリッジであることを知らせるために他のスイッチすべてに BPDU パケットを送信する間隔です。
Bridge Forward Delay **(4 - 30 Sec)**	**Forward Delay** に *4* から *30* 秒まで設定できます。ポートは Blocking から Forwarding に変更されるまでの間、設定された秒だけ Listening になります。
Bridge Priority (0-61440)	スイッチのプライオリティは *0* から *61440* まで設定できます。この数字はネットワーク上のスイッチ間の選出プロセスで使用され、どのスイッチがルートスイッチになるかを決定します。低い数字ほどプライオリティは高くなり、このスイッチがルートスイッチとして選出される可能性が高くなります。
Default Path Cost	ここは参照用のフィールドで、ポートごとのパスコストの初期値を決定するために使用するプロトコルを表示します。802.1T はポートの帯域に基づき決められた式を使用して 32 ビットコスト値を計算します。
STP Version	プルダウンメニューを使用し、STP のバージョンを設定します。 *STP Compatible* -スイッチ全体に Spanning Tree Protocol (STP)を設定します。 *RSTP* -スイッチ全体に Rapid Spanning Tree Protocol (RSTP) を設定します。
TX Hold Count (1-10)	送信間隔あたりに Hello パケットが送信される最大数を指定します。*1* から *10* までの値で設定できます。初期値は *3* です。
Forwarding BPDU	*Enabled* か *Disabled* を選択できます。*Enabled* ならば他のネットワークデバイスからの STP BPDU パケットを転送します。初期値は *Enabled* です。
LBP	この機能はスイッチにBPDU パケットが戻ってきた場合、スイッチ上の STP を一時的にブロックします。スイッチが自分自身の BPDU パケットが戻ってきたのを検出するということはネットワークが循環していることを示します。STP は自動的にブロックし、管理者にアラートを出します。**LBP Recover Time** がタイムアウトになるとLBD STP ポートは再スタート(discarding 状態に変更)します。プルダウンメニューを使用して、この機能を有効または無効にします。初期値は *Disabled* です。
LBD Recover Time	このフィールドには STP 状態を回復する前の STP ポートの待ち時間を設定します。*0* は管理者がその値を直接変更するまで LBD がタイムアウトにならず、再スタートしません。*60* から *1000000* 秒で設定できます。初期値は *60* 秒です。

Apply ボタンをクリックし、変更を適用します。

STP ポートの設定

ポートベースのSTPをポートに対して設定します。**Layer 2 Features > Spanning Tree > STP Port Settings**をクリックし、以下の画面を表示します。

Port	Connection	State	Cost	Priority	Edge	P2P	STP Status	Role	Port Forward BPDU	LBD
1	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
2	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
3	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
4	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
5	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
6	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
7	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
8	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
9	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
10	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
11	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
12	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
13	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
14	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
15	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
16	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
17	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
18	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
19	100M/Full/None	Yes	*2000000	128	No	Yes	Forwarding	NonStp	Enabled	No

図 7- 15. STP Port Settings と The STP Port Information 画面

スイッチレベルのスパニングツリーパラメータの設定に加えて、本スイッチはポートグループでスパニングツリーを構成し、必要に応じて固有の設定を行うことができます。STP グループはこれまでに設定したスイッチレベルのパラメータを使用しますが、さらに **Port Priority** と **Port Cost** についても加えて設定することができます。

STP グループのスパニングツリーはスイッチレベルでのスパニングツリーと同様に動作しますが、ルートブリッジの概念はルートポートの概念で置き換えられます。ルートポートはグループの中からプライオリティとポートコストに基づいて選ばれたポートでグループが動作するためにネットワークに接続します。スイッチレベルで冗長なリンクがブロックされるように、やはり冗長なリンクはブロックされます。

スイッチレベルの STP はスイッチ間(そして、ネットワークデバイス間も同様に)の冗長なリンクをブロックします。ポートレベルの STP は STP グループ内での冗長なリンクをブロックします。

STP グループのポートは VLAN グループと一致させておくことをお勧めします。

以下の項目について設定できます。

パラメータ	説明
From...To	設定する連続したポートグループの最初の番号と最後の番号を指定します。
Cost(0=Auto)	このポートにパケットを転送するためにかかるコストを表すメトリックを指定します。ポートのコストは自動か、メトリックの値で設定します。初期値は *0*(自動)です。 • *0* (自動) –選択ポートに可能な最良のパケット転送速度を自動的に設定します。ポートコストの初期値:100Mbps ポート = 200000、Gigabit ポート = 20000。 • 値 – *1* から *200000000* までの値で指定します。数字が低いほどパケット転送は頻繁に行われるようになります。
Priority	ポートプライオリティは *0* から *240* で指定します。低い数字ほどポートがルートポートに選ばれる可能性が高くなります。
Migration	このパラメータに"*Yes*"を設定すると、ポートは他のブリッジにそれらの STP 設定情報をリクエストしながら BPDU パケットを送信します。スイッチが RSTP 設定をしている場合、ポートは 802.1d STP から 802.1w RSTP へのプロトコルの移行が可能です。Migration はセグメントのすべてまたは一部に対して 802.1w に更新可能なネットワークステーションまたはネットワークセグメントに接続しているポートに *Yes* を設定します。
Edge	*True* パラメータを選ぶとポートはエッジポートになります。エッジポート自体は循環を発生させることはありませんが、トポロジーの変化によりループの可能性が生じる場合、エッジポートはエッジポートではなくなります。エッジポートは通常 BPDU パケットを受信しません。BPDU パケットを受信すると自動的にエッジポートではなくなります。*False* パラメータを選ぶとポートはエッジポートではなくなります。
P2P	*True* の場合、Point to point(P2P)ポートとしてリンクを共有します。P2P ポートはエッジポートと似ていますが、P2P ポートは全二重でなくてはならないという制限があります。P2P ポートはエッジポートのように RSTP による高速な転送状態の変更が可能です。*False* の場合、ポートは P2P 状態になることはありません。*Auto* の場合、可能であれば常に *True* と同様の P2P 状態になります。ポートが、例えば強制的に半二重になるなど状態を維持できない場合には、*False* と同様の状態になります。初期値は *True* です。
LBD	プルダウンメニューを使用して上記で指定したポートに対するスイッチのループバック検出機能を *Enabled*(有効)または *Disabled*(無効)にします。詳しくは **STP ループバック検出**を参照してください。

Apply ボタンをクリックし、変更を適用します。

確認: ポートごとに BPDU の転送を有効にするためには、はじめに以下の設定をしてください。:

1. STP はすべて *disabled*(無効)にします。
2. Forwarding BPDU の転送をすべて enabled(有効)にします。

これらは前述の **STP Bridge Global Settings** メニュー内にある初期設定です。

セクション 8

CoS

はじめに

本スイッチは 802.1p と別のプライオリティプロトコルをサポートしています。このセクションでは 802.1p priority queuing と Class of Service または CoS マッピングの使用について説明します。

IEEE 802.1p Priority

プライオリティタギングは多くの異なるデータを同時に転送するネットワーク上のトラフィックを管理するための IEEE 802.1p 規格に定義されている機能です。集中するネットワーク上でタイムクリティカルなデータ転送に関わる問題を緩和することが目的です。ビデオカンファレンス等タイムクリティカルなデータによるアプリケーションの品質は転送の少しの遅れでも大きく影響を受けます。

IEEE 802.1p 規格に準拠するネットワークデバイスは、データパケットのプライオリティレベルを認識する機能があります。これらのデバイスはパケットにプライオリティラベルとタグを割りあてることができます。準拠デバイスはさらにパケットからのプライオリティタグを取り除くこともできます。プライオリティタグはパケットの緊急度と割り当てるキューを決めます。

プライオリティタグは 0 から 7 までの値で指定し、0 がもっとも低いプライオリティで 7 がもっとも高いプライオリティです。もっともプライオリティが高い 7 は少しの遅れにも敏感なビデオやオーディオアプリケーションに関連するデータやデータ転送に特別な考慮を保証する必要がある特定のエンドユーザからのデータに通常使用されます。

本スイッチは、ご使用のネットワーク上でプライオリティタグのついたデータパケットの処理方法を細かく指定できます。プライオリティタグのついたデータを管理するキューを使用してご使用のネットワークの要求に合う相対的なプライオリティを指定できます。同じキュー内に 2 つ以上の異なるタグ付きパケットをグループ化することができます。しかし通常はもっとも高いプライオリティにはキュー3 を指定し、プライオリティ 7 はデータパケットのために取っておくことをお勧めします。プライオリティ値が設定されていないパケットはキュー0 に置かれ、送信のプライオリティはもっとも低くなります。

重み付けラウンドロビンシステムはどのキューのパケットを空にするかという割合を決定するために使用されます。キューをクリアするのに使用される比率は 4:1 です。これはキュー0 のパケットを 1 パケットクリアするごとにもっとも高いプライオリティのキュー3 が 4 つのパケットをクリアするという意味です。

スイッチのプライオリティキュー設定はスイッチに接続しているすべてのポートとデバイスに影響することに注意してください。ご使用のネットワークにプライオリティタグを割り当てることができるスイッチがある場合、プライオリティキューイングシステムは非常に有益なシステムです。

CoSのアドバンテージ

CoS は大きい帯域が必要か、または高い優先度を持つ重要な機能のために帯域を予約する手段をネットワーク管理者に提供する IEEE 802.1p 標準の機能です。帯域を予約するものには VoIP(voice-over Internet Protocol)、ウェブブラウジングアプリケーション、ファイルサーバアプリケーションまたはビデオ会議などがあります。より大きい帯域を作成可能なだけではなく他の重要度の低いトラフィックを制限することで、ネットワークが必要以上の帯域使用しないようにします。スイッチは各物理ポートで受信した様々なアプリケーションからのパケットをプライオリティに基づき独立したハードウェアキューに振り分けます。以下の図は基本的な 802.1P プライオリティキューイングです。

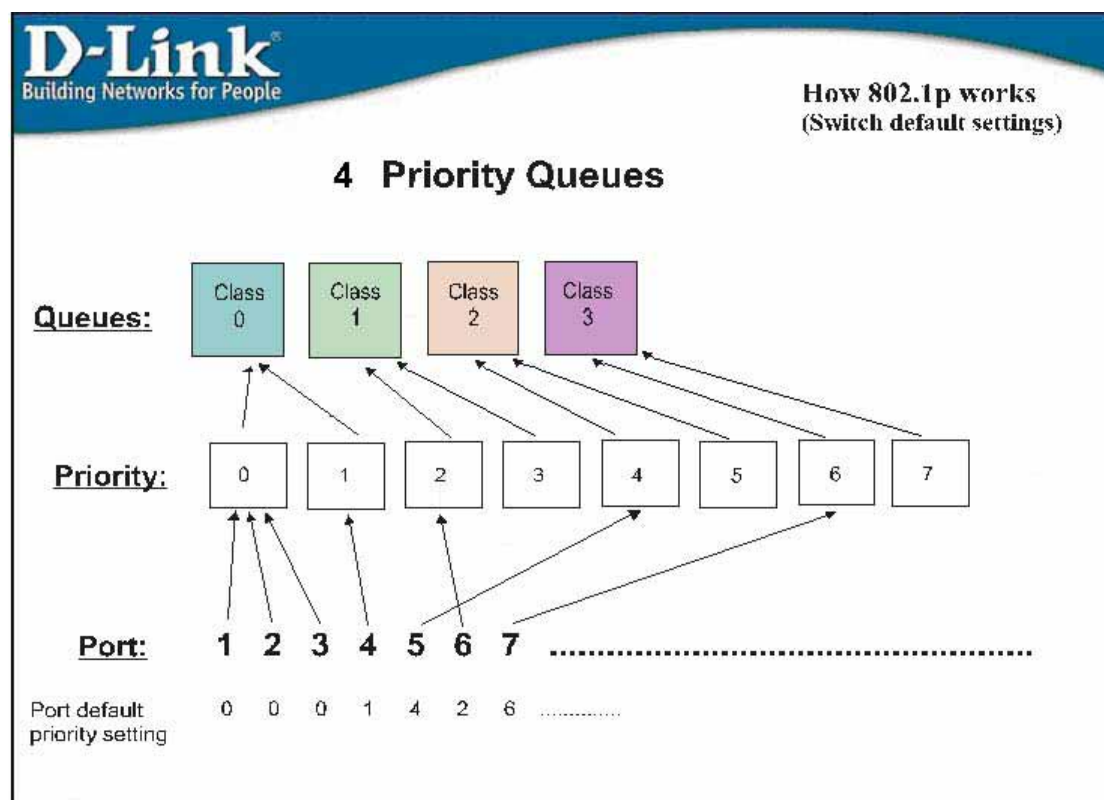



図 8- 1. 本スイッチにおけるデフォルトの CoS 振り分けの例

上の図は本スイッチのプライオリティの初期設定です。Class-3 は本スイッチの持つ 4 つのサービスクラスのプライオリティの中で最も高いプライオリティです。CoS を実行するために、パケットヘッダが正常な識別タグを持っているとスイッチがそれを調査します。次に、これらのサービスクラスのタグ付けをされたパケットをプライオリティに基づき処理します。

例えば、二つの離れたコンピュータを使用しビデオ会議を行うとします。管理者はアクセスプロファイルコマンドを使用し、ビデオパケットにプライオリティタグを付け、送信します。そして、受信側では管理者がこのタグを調べタグ付パケットを特定のクラスキューに振り分けるように設定します。次に、管理者はこのキューに「他のどんなパケットが転送されるよりも前に空にする」という優先度を設定します。これによりエンドユーザはすべてのパケットを可能な限り早く受け取ることができ、キューに対するプライオリティが付き、パケットストリームを分割できないビデオ会議などで使用するための帯域の最適化が行われます。

CoSについて

本スイッチは 802.1p priority queuing をサポートしています。本スイッチは 4 つのプライオリティクラスを持っています。これらのプライオリティクラスは、もっともプライオリティの高いキューの 3(Class 3)から、もっともプライオリティの低い 0(Class 0)までの数字が振られています。IEEE 802.1p で規定されている p0 から p7 までの 8 つのプライオリティクラスは本スイッチでは以下のように割り当てられています。

プライオリティ 0 はスイッチの Q1 クラスに割り当てられています。

プライオリティ 1 はスイッチの Q0 クラスに割り当てられています。

プライオリティ 2 はスイッチの Q0 クラスに割り当てられています。

プライオリティ 3 はスイッチの Q1 クラスに割り当てられています。

プライオリティ 4 はスイッチの Q2 クラスに割り当てられています。

プライオリティ 5 はスイッチの Q2 クラスに割り当てられています。

プライオリティ 6 はスイッチの Q3 クラスに割り当てられています。

プライオリティ 7 はスイッチの Q3 クラスに割り当てられています。

プライオリティスケジューリングは Strict プライオリティとランドロビンプライオリティの2つの方式を使用して行います。CoS プライオリティスケジューリング設定に変更がない場合、使用される方式は Strict プライオリティとなります。

Strict プライオリティベースのスケジューリングでは、最も高い CoS に属するパケットがはじめに転送されます。一度 CoS に対して Strict スケジューリングが実行されると、もっともプライオリティの高いクラスは Strict モードで動作し、他のクラスは適正な重み付けのスケジューリングモードにとどまります。バッファ内ではより低いプライオリティパケット量でより低いプライオリティパケットが転送されてから時間が経過しているにもかかわらず高いプライオリティパケットほどいつも優先権を受け取ります。初期値では Strict プライオリティを使用してバッファを空にする設定になっています。

注意: CoS スケジューリング設定の初期値は Strict プライオリティスケジュールです。これは他のキューがラウンドロビン方式で空とされている間はもっとも高い CoS が Strict スケジューリングだけを持っているとスイッチが見なすことを意味します。詳しい情報については「CoS スケジューリングメカニズム」を参照してください。

重み付けラウンドロビンプライオリティを使用するために、本スイッチの４つのプライオリティサービスクラスは round-robin fashion 内のバッファを減少させるように設定できます。もっともプラオリティが高いサービスクラスではじまり、もっともプライオリティが高いサービスクラスに戻る前にもっともプライオリティが低い CoS に移行します。

重み付けプライオリティベースのスケジューリングは Strict ベースのスケジューリングの主な欠点を緩和します。例えばより低いプライオリティのサービスクラスでは帯域の枯渇をすべてのサービスクラスに対して最小の帯域を供給することで緩和します。これはプライオリティを付与されたサービスクラスから転送を許可されるパケットの最大数とプライオリティを付与されたサービスクラスが蓄積したパケット転送の許可前に待機する必要がある最大時間を設定することで実行されます。スイッチの４つのプライオリティサービスクラスのそれぞれに Class of Service (CoS)を確立します。

可能な重み付けの範囲は 1 から 55 パケットです。

代わりのプライオリティプロトコルを使用するネットワーク環境では、スイッチの CoS を DSCP プライオリティや Type of Service (ToS)プライオリティに適応させるためにマッピングすることができます。CoS はまた指定したスイッチの送信先 MAC アドレスやポートにマップすることができます。

Command Line Interface Reference Manual で CoS コマンドがパラメータとともに記載されています。

帯域制御

帯域制御の設定を行うことにより選択ポートへの送信と受信のデータレートを制限することができます。**CoS > Port Bandwidth** をクリックし、以下の画面を表示します。

図 8- 2. Bandwidth Settings と Port Bandwidth Table 画面

以下のパラメータを設定、確認できます。

パラメータ	説明
From...To	設定を行うポートの連続した範囲を指定します。
Type	ドロップダウンメニューを使用して *RX* (受信)、*TX* (送信)および *Both*(両方)から選択します。帯域上限を受信、送信、受送信の両方のいずれに適用するのかを設定します。
no_limit	選択ポートに対して帯域制限を行うかを設定します。*Enabled* にすると制限がなくなります。
Rate	データレートの制限値を Kbit/s 単位で指定します。*64* から *1024000*Kbit/s で指定します。

Apply ボタンをクリックし、選択ポートの帯域制御を設定します。設定の結果は **Port Bandwidth Table** に表示されます。

802.1p デフォルトプライオリティ

本スイッチは各ポートにデフォルトの 802.1p プライオリティを割り当てることができます。**CoS > 802.1p Default Priority** とクリックし、以下の画面を表示します。

図 8- 3. Port Default Priority assignment と The Port Priority Table 画面

この画面ではそれぞれのポートにデフォルトの802.1pプライオリティを割り当てます。プライオリティタグは最低の0から最高の7まで指定できます。新しいデフォルトプライオリティを割り当てるには**From**と**To**でポートの範囲を指定して、**Priority**に0から7を指定します。**Apply**ボタンをクリックし、変更を適用します。

802.1p ユーザプライオリティ

本スイッチはそれぞれのサービスクラスに802.1pプライオリティを割り当てることができます。**CoS > 802.1p User Priority**とクリックし、以下の画面を表示します。

図 8- 4. User Priority Configuration 画面

ポートに割り当てた7段階のプライオリティに対してクラスを設定します。**Apply**ボタンをクリックし、変更を適用します。

CoS スケジューリングメカニズム

このドロップダウンメニューよりプライオリティクラスを処理する手法として **Weight Fair** と **Strict** のどちらかを選びます。**CoS > CoS Scheduling Mechanism** とクリックし、以下の画面を表示します。

図 8- 5. CoS Scheduling Mechanism と CoS Scheduling Mechanism Table 画面

注意: CoS スケジューリング設定の初期値は Strict プライオリティスケジュールです。これは他のキューがラウンドロビン方式で空とされている間はもっとも高いクラス(Class-3)が Strict スケジューリングだけを持っているとスイッチが見なすことを意味します。

Scheduling Mechanism には以下のパラメータがあります。

パラメータ	説明
Strict	Strict スケジューリングがもっとも高いキューに設定されると、他のキューが重み付けラウンドロビンスケジューリング体系に従っているあいだははじめに処理されることを表しています。
weight fair	プライオリティのサービスクラスで配分されたパケットを重み付けされたラウンドロビン(*WRR*)アルゴリズムによって処理します。

Apply をクリックし、変更を適用します。

CoS の送出スケジューリング

CoS はハードウェアサービスクラスを使用することによって送出スケジューリングを変更できます。CoS の設定に何らかの変更を加える場合、低いプライオリティのサービスクラスのネットワークトラフィックがどのように影響を受けるのか注意深く検討する必要があります。スケジューリングの変更は予期せぬパケットロスや重大な転送遅延を引き起こすことがあります。設定の変更をするときには特にピーク時に必要な帯域に注意してネットワークパフォーマンスを監視し、CoS の設定が適切でない場合、速やかにボトルネックを見つけることが大事です。**CoS > CoS Output Scheduling** とクリックし、以下の画面を表示します。

図 8- 6. CoS Output Scheduling 設定画面

CoS クラスのスケジューリングには以下の値を設定できます。

パラメータ	説明
Weight	次にプライオリティが低いキューが送信するまでに、該当するハードウェアプライオリティサービスクラスが送信することのできるパケットの最大数を指定します。*0* から *55* を指定します。

Applyボタンをクリックし、変更を適用します。

プライオリティ設定

CoS > Priority Settings とメニューをクリックし、以下の画面を表示します

図 8- 7. Priority Setting

Priority Setting パラメータは以下のとおりです。

パラメータ	説明
From..To	設定を行うポートの連続した範囲を指定します。
Main Select	設定ポートの通常のプライオリティ設定を選択します。プライオリティオプションは次のとおりです。: **port_priority** – ポートベースのプライオリティ **802.1p_priority** – 802.1p プライオリティ **mac_base** – MAC ベースプライオリティ **tos** –TOS-IP **dscp** – または DSCP-IP **none** – プライオリティ設定なし

Applyボタンをクリックし、変更を適用します。

TOS プライオリティ設定

TOS Priority Setting メニューを使用して、スイッチ上のサービスクラスに対する ToS プライオリティマッピングを設定します。**CoS > TOS Priority Settings** とメニューをクリックし、以下の画面を表示します。

図 8- 8. TOS Priority Setting

プルダウンメニューより **TOS** の値とマップされる **Class ID** を選択して **Apply** ボタンをクリックします。新しいマッピングが以下の **Port Priority Table** 内に表示されます。

DSCP プライオリティ設定

DSCP Priority Setting メニューを使用してスイッチ上に CoS の DSCP プライオリティマッピングを設定します。

CoS > DSCP Priority Settings とメニューをクリックし、以下の画面を表示します。

図 8- 9. DSCP Priority Setting

マップされる **DSCP** ビットレベルとプルダウンメニューより **Class ID** を指定し、**Apply** ボタンをクリックします。ます。新しいマッピングは以下の **DSCP Priority Table** に表示されます。

ポートマッピングプライオリティ設定

CoS > Port Mapping Priority Settings とメニューをクリックし、以下の画面を表示します。**Port Mapping Priority CoS** を使用するためには **Priority Setting** メニュー内の選択ポートの設定をします。2つのサービスクラスを設定できます。

図 8- 10. Port Mapping Priority CoS

From/To メニューを使用して設定されるポートを選択します。選択ポートには Priority Setting メニューでポートベースのプライオリティをはじめに設定する必要があります。ポートに **Class** レベルを選択します。Class レベルには高プライオリティには 3、低プライオリティには 0 の2つがあります。

MAC プライオリティ設定

CoS > Mac Priority とメニューをクリックし、以下の画面を表示します。**MAC Setting** メニューを使用して特定の送信先 MAC アドレスへのサービスクラスレベルを割り当てます。

図 8- 11. MAC Priority Setting

MAC Address を入力し、**Class ID** を選択して **Apply** ボタンをクリックします。

セクション 9

CPUインタフェースフィルタリング

チップセットの制限やスイッチのセキュリティの必要性などから本スイッチは CPU インタフェースフィルタリング機能を持っています。この追加機能によって CPU インタフェース向けのパケットアクセスルールリストの作成が可能になり、動作時のセキュリティが高くなります。CPU インタフェースフィルタリングはイーサネット、IP とパケットの内容、CPU 向けにマスクされたパケットヘッダを調べて、ユーザ設定に基づきそれらを転送もしくはフィルタリングします。そして CPU フィルタリング向けの追加機能として、本スイッチの CPU フィルタリング手法では多彩なルールのリストをあらかじめ用意しておき、必要に応じて全体に対して有効/無効を設定することができます。

CPU用のアクセスプロファイルの作成は2段階に分かれます。はじめにフレームのどの部分を調べるのか、送信元MACアドレスか、送信先IPアドレスか、などを決定します。次に、そのフレームに対してどのような処理を行うのかという基準になる値を入力します。詳しくは以下で2つに分けて説明します。

CPU インタフェースフィルタリング状態の設定

以下の画面で CPU インタフェースフィルタリングの有効/無効をプルダウンメニューで切り替えることができます。この画面は **CPU Interface Filtering > CPU Interface Filtering State** とクリックし、以下の画面を表示します。**Enabled** を選ぶと CPU パケットは検査され、**Disabled** を選ぶと検査は中止されます。

図 9- 1. CPU Interface Filtering State Settings 画面

CPU インタフェースフィルタリングテーブル

CPU Interface Filtering Table は作成された CPU アクセスプロファイルテーブルのエントリを表示します。**CPU Interface Filtering > CPU Interface Filtering Table** とクリックし、以下の画面を表示します。エントリの設定を見るためには **Profile ID** 番号のハイパーリンクをクリックします。

図 9- 2. CPU Interface Filtering Table

CPU Interface Filtering Table にエントリを追加するには **Add** ボタンをクリックします。以下の **CPU Interface Filtering Configuration** 画面が表示されます。**CPU Interface Filtering Configuration** 画面には以下の 4 種類があります。イーサネット(MAC アドレスベース)プロファイル設定、IP アドレスベースのプロファイル設定、そして、パケット内容のマスク設定です。 この 4 種類の **CPU Interface Filtering Configuration** 画面は **Type** のドロップダウンメニューで切り替えることができます。以下はイーサネットの **CPU Interface Filtering Configuration** 画面です。

CPU Interface Filtering Configuration

Profile ID(1-3)	1
Type	Ethernet
Vlan	
Source Mac	00-00-00-00-00-00
Destination Mac	00-00-00-00-00-00
802.1p	
Ethernet type	

Apply

Show All CPU Interface Filtering Table Entries

図 9- 3. CPU Interface Filtering Configuration 画面 – Ethernet

パラメータ	説明
Profile ID (1-3)	プロファイルのための固有の識別番号を指定します。*1* から *3* で指定できます。
Type	*Ethernet*(MAC アドレス)、*IP*、*Packet Content Mask* の中からプロファイルのベースを指定します。**Type** の変更に伴いメニューも変わります。 • *Ethernet*を選ぶとパケットヘッダのレイヤ2部分を対象にします。 • *IP*を選ぶとフレームヘッダのIPアドレスを対象にします。 • *Packet Content Mask*を選ぶとパケットヘッダの内容をマスクして隠します。
Vlan	このオプションを指定するパケットヘッダの VLAN 識別子を調べて、部分的もしくは全体を転送基準として使用します。
Source Mac	Source MAC のマスク - 送信元 MAC アドレスをマスクする MAC アドレスを指定します。
Destination Mac	Destination MAC のマスク - 送信先 MAC アドレスをマスクする MAC アドレスを指定します。
802.1p	このオプションを指定するとフレームヘッダで 802.1p タイプの値を調べます。
Ethernet type	このオプションを指定するとフレームヘッダでイーサネットタイプの値を調べます。

このエントリをスイッチに保存するには **Apply** ボタンをクリックします。

以下は **CPU Interface Filtering Configuration** 画面です。

CPU Interface Filtering Configuration
Profile ID(1-3) 1
Type IP
Vlan
Source IP Mask 0.0.0.0
Destination IP Mask 0.0.0.0
Dscp
Protocol ICMP type code
IGMP type
TCP src port mask 0000
dest port mask 0000
flag mask bit
urg ack psh
rst syn fin
UDP src port mask 0000
dest port mask 0000
protocol id user mask 00000000
Apply
Show All CPU Interface Filtering Table Entries

図 9- 4. CPU Interface Filtering Configuration 画面- IP

パラメータ	説明
Profile ID (1-3)	プロファイルのための固有の識別番号を指定します。*1* から *3* で指定できます。
Type	*Ethernet*(MAC アドレス)、*IP*、*Packet Content Mask* の中からプロファイルのベースを指定します。**Type** の変更に伴いメニューも変わります。 • *Ethernet*を選ぶとパケットヘッダのレイヤ2部分を対象にします。 • *IP*を選ぶとフレームヘッダのIPアドレスを対象にします。 • *Packet Content Mask*を選ぶとパケットヘッダの内容をマスクして隠します。
VLAN	このオプションを指定するパケットヘッダの VLAN 識別子を調べて、部分的もしくは全体を転送基準として使用します。
Source IP Mask	送信元 IP アドレスをマスクする IP アドレスを指定します。
Destination IP Mask	送信先 IP アドレスをマスクする IP アドレスを指定します。
Dscp	このオプションを指定すると各パケットヘッダの DiffServ コードを調べて、部分的もしくは全体を転送基準として使用します。
Protocol	このオプションを指定するとそれぞれのフレームヘッダのプロトコルタイプを調べます。転送基準にどのようなプロトコルを含めるかを指定します。

<table>
<tr><td></td><td>
ICMP を選ぶと各フレームヘッダの Internet Control Message Protocol(ICMP)フィールドを調べます。
Type を選ぶと ICMP タイプの値を、Code を選ぶと ICMP コードの値を適用します。
IGMP を選ぶとそれぞれのフレームヘッダの Internet Group Management Protocol (IGMP)フィールドを調べます。
Type を選ぶと IGMP タイプの値を適用することになります。
TCP を選ぶと転送基準となる受信パケットの TCP ポート番号を使用します。TCP を選ぶと送信元ポートマスク(source port mask)と(もしくは)送信先ポートマスク(dest port mask)を指定する必要があります。フラグビット(flag bit)をフィルタに使用することもできます。flag bit はパケットがどのような振る舞いをするかを決定するパケットの一部です。パケットの flag bit でフィルタリングするには TCP フィールドの flag bit に一致する内容のボックスをチェックします。urg (urgent)、ack (acknowledgement)、psh (push)、rst (reset)、syn (synchronize)、fin (finish)を選ぶことができます。
src port mask - フィルタリングしたい送信元ポートをマスクする TCP ポートを 16 進数(hex 0x0-0xffff)で指定します。
dst port mask - フィルタリングしたい送信先ポートをマスクする TCP ポートを 16 進数(hex 0x0-0xffff)で指定します。
UDPを選ぶと、転送基準となる受信したパケットの UDP ポート番号を使用します。UDP を選ぶと送信元ポートマスク(source port mask)と(もしくは)送信先ポートマスク(dest port mask)を指定する必要があります。
src port mask - フィルタリングしたい送信元ポートをマスクする UDP ポートを 16 進数(hex 0x0-0xffff)で指定します。
dst port mask - フィルタリングしたい送信先ポートをマスクする UDP ポートを 16 進数(hex 0x0-0xffff)で指定します。
protocol id - マスクしたいパケットヘッダの protocol ID を指定します。Protocol ID マスクは 16 進数(hex 0x0-0xffffffff)で指定します。
</td></tr>
</table>

このエントリをスイッチに保存するためには **Apply** ボタンをクリックします。

以下は **CPU Packet Content Configuration** 画面です。

CPU Interface Filtering Configuration				
Profile ID(1-3	1			
Type	Packet Content			
Offset_0-15	☐	00000000 00000000	00000000	00000000
Offset_16-31	☐	00000000 00000000	00000000	00000000
Offset_32-47	☐	00000000 00000000	00000000	00000000
Offset_48-63	☐	00000000 00000000	00000000	00000000
Offset_64-79	☐	00000000 00000000	00000000	00000000
				Apply

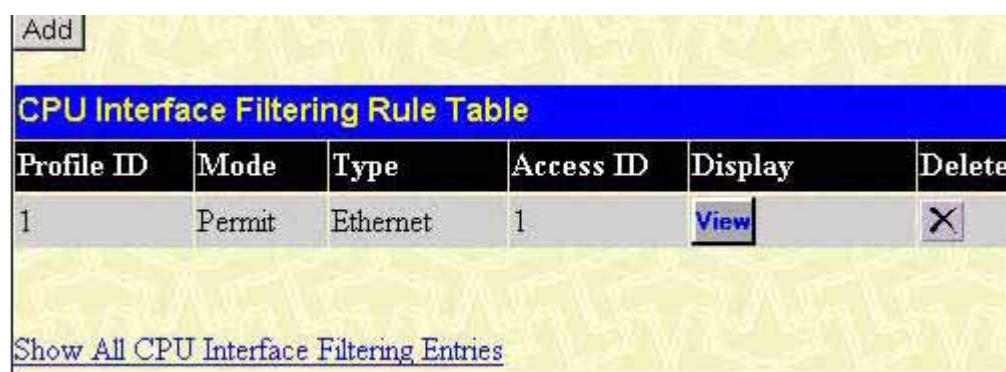
Show All CPU Interface Filtering Table Entries

図 9- 5. CPU Interface Filtering Configuration 画面- Packet Content

この画面ではパケットヘッダにマスクを開始するオフセットを指定します。**Packet Content** マスクでは以下のフィールドが設定できます。

パラメータ	説明
Profile ID (1-3)	プロファイルのための固有の識別番号を指定します。*1* から *3* で指定できます。
Type	*Ethernet*(MAC アドレス)、*IP*、*Packet Content Mask* の中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。 • *Ethernet*を選ぶとパケットヘッダのレイヤ2部分を対象にします。 • *IP*を選ぶとフレームヘッダのIPアドレスを対象にします。 • *Packet Content Mask*を選ぶとパケットヘッダの内容をマスクして隠します。
Offset	パケットヘッダにマスクを開始するオフセットを指定します。 • *value (0-15)* - 16進数でパケットの最初から15バイト目までのマスクを指定します。 • *value (16-31)* – 16進数でパケットの16バイト目から31バイト目までのマスクを指定します。 • *value (32-47)* – 16進数でパケットの32バイト目から47バイト目までのマスクを指定します。 • *value (48-63)* – 16進数でパケットの48バイト目から63バイト目までのマスクを指定します。 • *value (64-79)* – 16進数でパケットの64バイト目から79バイト目までのマスクを指定します。

Apply ボタンをクリックし、変更を適用します。

作成した **CPU** アクセスプロファイルに対するルールの設定手順:

CPU Interface Filtering > CPU Interface Filtering Table とクリックし、**CPU Interface Filtering Table** を表示します。

Add

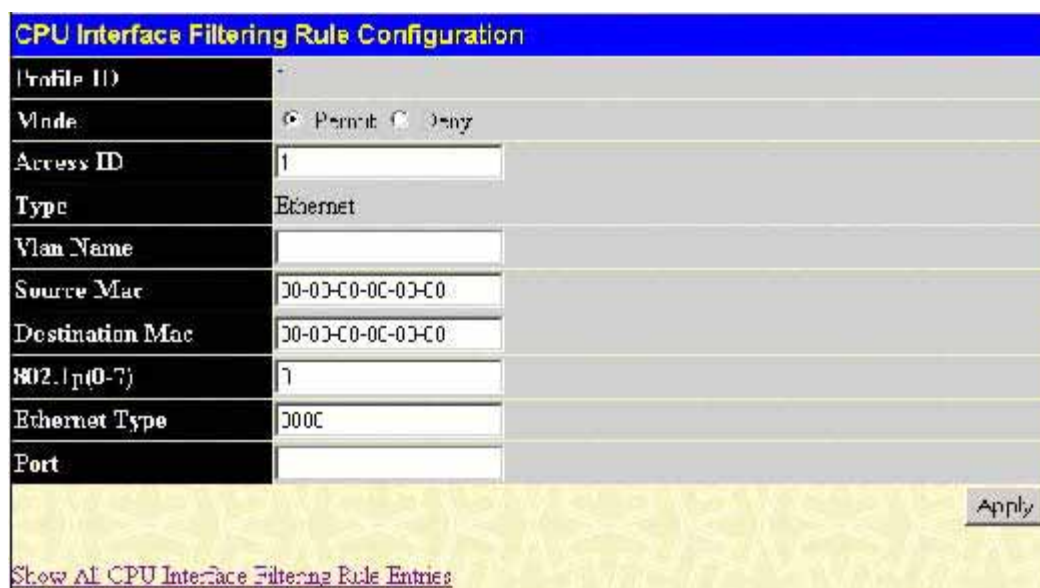
CPU Interface Filtering Table

Profile ID	Type	Access Rule	Delete
1	Ethernet	Modify	X
2	IP	Modify	X
3	Packet Content	Modify	X

図 9- 6. CPU Interface Filtering Table

この画面で **Modify** ボタンをクリックすると CPU アクセスプロファイルに対応した **Ethernet**、**IP** または **Packet Content** の新しいルールを設定することができます。それぞれのエントリは以下の画面で行います。

Add

CPU Interface Filtering Rule Table

Profile ID	Mode	Type	Access ID	Display	Delete
1	Permit	Ethernet	1	View	X

Show All CPU Interface Filtering Entries

図 9- 7. CPU Interface Filtering Table – Ethernet

アクセスプロファイルに対応した新しいルールセットを作るには **Add** ボタンをクリックし、新しい画面を表示します。すでに作成したルールを削除するには対応する ボタンをクリックします。以下の画面では Ethernet ルールを設定します。

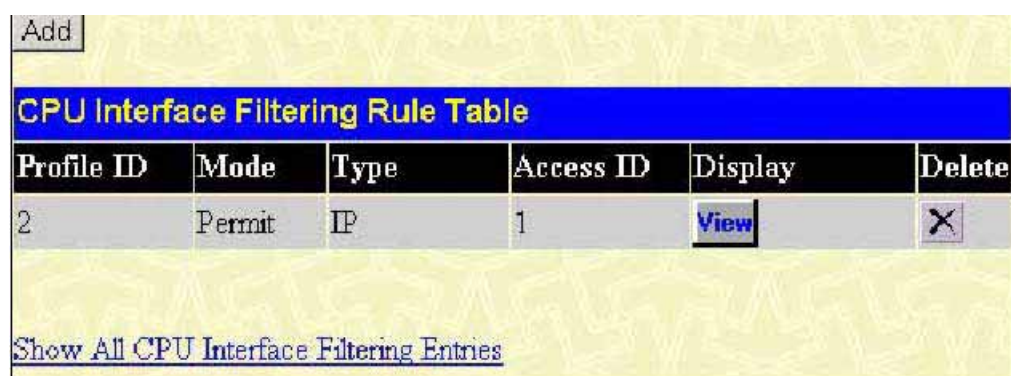
CPU Interface Filtering Rule Configuration

Profile ID	
Mode	Permit / Deny
Access ID	1
Type	Ethernet
Vlan Name	
Source Mac	00-00-00-00-00-00
Destination Mac	00-00-00-00-00-00
802.1p(0-7)	0
Ethernet Type	0000
Port	

Apply

Show All CPU Interface Filtering Rule Entries

図 9- 8. CPU Interface Filtering Rule Configuration – Ethernet

Ethernetのアクセスルールを設定するには以下のパラメータを設定し、**Apply**ボタンをクリックします。

パラメータ	説明
Profile ID	プロファイルのための固有の識別番号です。
Mode	*Permit* を選ぶとアクセスプロファイルにマッチしたパケットを転送します。このとき新しいルールが追加されることもあります(以下参照)。 *Deny* を選ぶとアクセスプロファイルにマッチしたパケットは転送せずにをフィルタリングします。
Access ID	それぞれのルールに固有の番号を指定します。*1* から *5* で指定できます。
Type	プロファイルのベースが表示されます。 • *Ethernet*を選ぶとパケットヘッダのレイヤ2部分を対象にします。 • *IP*を選ぶとフレームヘッダのIPアドレスを対象にします。 • *Packet Content Mask*を選ぶとパケットヘッダの内容をマスクして隠します。
VLAN Name	すでに構成されている VLAN 名を指定します。
Source MAC	送信元 MAC アドレス - 送信元 MAC アドレスをマスクする MAC アドレスを指定します。
Destination MAC	送信先 MAC アドレス - 送信先 MAC アドレスをマスクする MAC アドレスを指定します。
802.1p (0-7)	アクセスプロファイルが適用されるパケットヘッダの 802.1p プライオリティを指定します。
Ethernet Type	アクセスプロファイルが適用されるパケットヘッダの 802.1Q イーサネットタイプの値を 16 進数(hex 0x0-0xffff)で指定します。イーサネットタイプは次の形式で指定します。: hex 0x0-0xffff。(a-f の半角英文字と *0-9999* の数字)
Port	アクセスルールが設定されるポート番号を指定します。

すでに設定されているルールを参照するためには、**CPU Interface Filtering Rule Table**で View をクリックし、以下の画面を表示します。

CPU Interface Filtering Rule Display	
Profile ID	1
Access ID	1
Mode	Permit
Type	Ethernet
Vlan Name	default
Source Mac	------
Destination Mac	------
802.1p	------
Ethernet Type	------
Activate State	Enabled
Port	8

Show All CPU Interface Filtering Rule Entries

図 9- 9. CPU Interface Filtering Rule Display – Ethernet

以下の画面は IP に対する **CPU Interface Filtering Rule Table** です。

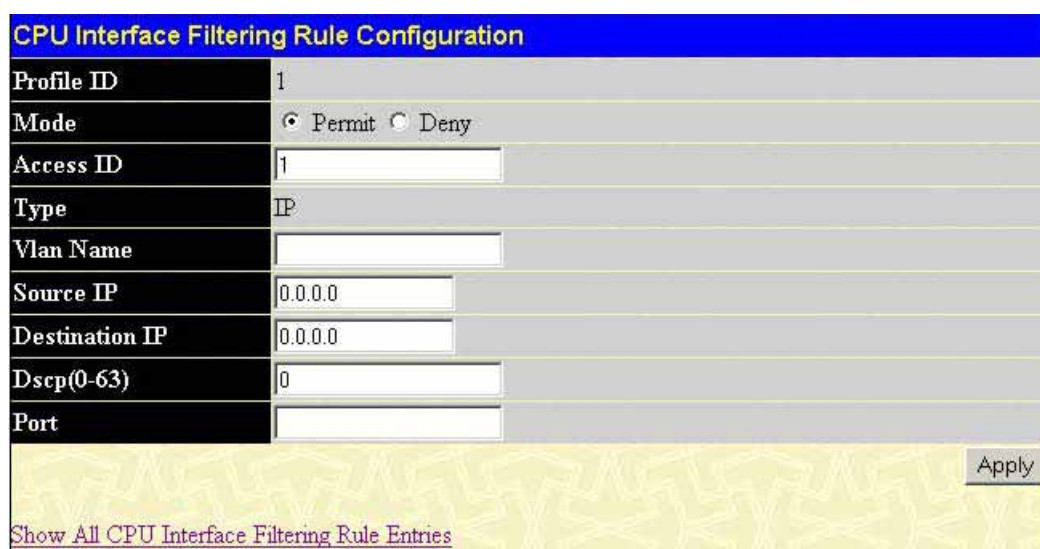



図 9- 10. CPU Interface Filtering Rule Table – IP

アクセスプロファイルに対応した新しいルールセットを作るには **Add** ボタンをクリックし、新しい画面を表示します。すでに作成したルールを削除するためには対応する ボタンをクリックします。以下の画面では IP ルールを設定します。

図9- 11. CPU Interface Filtering Rule Configuration – IP

以下はIPに対する **Access Rule Configuration**設定のパラメータです。

パラメータ	説明
Profile ID	プロファイルのための固有の識別番号です。
Mode	*Permit* を選ぶとアクセスプロファイルにマッチしたパケットを転送します。このとき新しいルールが追加されることもあります(以下参照)。 *Deny* を選ぶとアクセスプロファイルにマッチしたパケットは転送せずにをフィルタリングします。
Access ID	それぞれのルールに固有の番号を指定します。*1* から *5* で指定できます。
Type	プロファイルのベースが表示されます。 *Ethernet* を選ぶとパケットヘッダのレイヤ 2 部分を対象にします。 *IP* を選ぶとフレームヘッダの IP アドレスを対象にします。 *Packet Content Mask* を選ぶとパケットヘッダの内容をマスクして隠します。
VLAN Name	すでに設定している VLAN 名を指定します。

Source IP	送信元 IP アドレス - 送信元 IP アドレスをマスクする IP アドレスを指定します。
Destination IP	送信先 IP アドレス - 送信先 IP アドレスをマスクする IP アドレスを指定します。
Dscp (0-63)	このオプションを指定するとそれぞれのパケットヘッダの DiffServ コードを調べて、部分的もしくは全体を転送基準として使用します。*0* から *63* で指定できます。
Port	アクセスルールはこのフィールドにスイッチのポート番号ベースで設定します。*all* はスイッチのポートすべてを表します。

すでに設定されているルールを参照するためには **CPU Interface Filtering Rule Table** で View をクリックし、以下の画面を表示します。

CPU Interface Filtering Rule Display

Profile ID	1
Access ID	1
Mode	Permit
Type	IP
Vlan Name	default
Source IP	------
Destination IP	------
Dscp	------
Protocol	------
Activate State	Enabled
Port	

Show All CPU Interface Filtering Rule Entries

図 9- 12. CPU Interface Filtering Rule Display – IP

以下の画面は Packet Content の **CPU Interface Filtering Rule Table** です。

Add

CPU Interface Filtering Rule Table

Profile ID	Mode	Type	Access ID	Display	Delete
3	Permit	Packet Content	1	View	X

Show All CPU Interface Filtering Entries

図 9- 13. CPU Interface Filtering Rule Table – Packet Content

アクセスプロファイルに対応した新しいルールセットを作るには **Add** ボタンをクリックし、新しい画面を表示します。すでに作成したルールを削除するためには対応する ボタンをクリックします。

図 9- 14. CPU Interface Filtering Rule Configuration - Packet Content

Packet Content のアクセスルールを指定するには以下のパラメータを設定して、**Apply** ボタンをクリックします。

パラメータ	説明
Profile ID	プロファイルのための固有の識別番号です。
Mode	*Permit* を選ぶとアクセスプロファイルにマッチしたパケットを転送します。このとき新しいルールが追加されることもあります(以下参照)。 *Deny* を選ぶとアクセスプロファイルにマッチしたパケットは転送せずにをフィルタリングします。
Access ID	それぞれのルールに固有の番号を指定します。*1* から *5* で指定できます。
Type	プロファイルのベースが表示されます。 • *Ethernet*を選ぶとパケットヘッダのレイヤ2部分を対象にします。 • *IP*を選ぶとフレームヘッダのIPアドレスを対象にします。 • *Packet Content Mask*を選ぶとパケットヘッダの内容をマスクして隠します。
Offset	パケットヘッダにマスクを開始するオフセットを指定します。 • *value (0-15)* - 16進数でパケットの最初から15バイト目までのマスクを指定します。 • *value (16-31)* – 16進数でパケットの16バイト目から31バイト目までのマスクを指定します。 • *value (32-47)* – 16進数でパケットの32バイト目から47バイト目までのマスクを指定します。 • *value (48-63)* – 16進数でパケットの48バイト目から63バイト目までのマスクを指定します。 • *value (64-79)* – 16進数でパケットの64バイト目から79バイト目までのマスクを指定します。
Port	アクセスルールはこのフィールドにスイッチのポート番号ベースで設定します。*all* はスイッチのポートすべてを表します。

すでに設定されているルールを参照するためには **CPU Interface Filtering Rule Table** 画面で をクリックし、以下の画面を表示します。

図 9- 15. CPU Interface Filtering Rule Display – Packet Content

セクション 10

セキュリティ

トラフィックコントロール

ポートセキュリティ

ポートロックエントリ

802.1X認証の設定

トラストホスト

トラフィックセグメンテーション

本セクションではスイッチのセキュリティ機能の設定方法を説明します。本スイッチにはセキュリティ機能として *Traffic Control*、*Port Security*、*802.1X*、*Trusted Host* および *Traffic Segmentation* があり、続く各セクションで詳しく説明します。

トラフィックコントロール

ストームコントロールの有効/無効や、マルチキャストやブロードキャストのしきい値の調整、DLF(Destination Look Up Failure)を設定するには**Traffic Control**メニューを使用します。トラフィックコントロール設定はそれぞれのスイッチモジュールに適用されます。**Security > Traffic Control** とクリックし、以下の画面を表示します。

Traffic Control Settings

From	To	Broadcast Storm	Multicast Storm	Destination Lookup Fail	Threshold	Apply
Port 1	Port 1	Disabled	Disabled	Disabled	128	Apply

Traffic Control Table

Port	Broadcast Storm	Multicast Storm	Destination Lookup Fail	Threshold (Kbit/sec)
1	Disabled	Disabled	Disabled	64
2	Disabled	Disabled	Disabled	64
3	Disabled	Disabled	Disabled	64
4	Disabled	Disabled	Disabled	64
5	Disabled	Disabled	Disabled	64
6	Disabled	Disabled	Disabled	64
7	Disabled	Disabled	Disabled	64
8	Disabled	Disabled	Disabled	64
9	Disabled	Disabled	Disabled	64
10	Disabled	Disabled	Disabled	64
11	Disabled	Disabled	Disabled	64
12	Disabled	Disabled	Disabled	64
13	Disabled	Disabled	Disabled	64
14	Disabled	Disabled	Disabled	64
15	Disabled	Disabled	Disabled	64
16	Disabled	Disabled	Disabled	64
17	Disabled	Disabled	Disabled	64
18	Disabled	Disabled	Disabled	64

図 10- 1. Traffic Control Settings と Traffic Control Table 画面

Traffic Control を設定するためには、はじめに **From/To** プルダウンを使用してポートグループの選択をします。最後に対応するプルダウンメニューを使用して **Broadcast Storm**、**Multicast Storm** および **Destination Unknown** を有効または無効にします。

この画面はネットワークを取り囲む多くのブロードキャスト、マルチキャストまたは未知のユニキャストを制限します。各ポートは 1 秒あたりに受信するブロードキャスト量を確認するカウンタを持っており、このカウンタは 1 秒ごとにクリアされます。**Broadcast Storm**、**Multicast Storm** または **Destination Unknown** 設定が有効である場合、カウンタが指定の **Threshold** 値以上になるとポートに受信したすべてのブロードキャスト、マルチキャストまたは未知のユニキャストを破棄します。

Threshold 値はしきい値であり、これを超えると指定したトラフィックコントロールが実行されます。ストームトラフィックコントロール量をトリガーとするスイッチが受信するブロードキャスト、マルチキャストまたは DLF トラフィック量を Kbps (1 秒あたりのキロビット数)で表します。**Threshold** 値は 64 から 1024000Kbps/秒で指定します。初期値は 64 です。各ポートの設定は同じ画面の **Traffic Control Table** で参照できます。**Apply** ボタンをクリックし、設定を有効にします。

ポートセキュリティ

指定したポートのダイナミックな MAC アドレスの学習をロックすることができます。すなわち、ポートロックが有効になると MAC アドレス送信テーブルに登録された送信元 MAC アドレスは変更されることはありません。**Security > Port Security** をクリックし、以下の **Port Security Setting** 画面を表示します。**Admin State** プルダウンメニューで *Enabled* を選び、**Apply** ボタンをクリックし、ポートをロックします。

Port Security というセキュリティ機能を使用するとスイッチのポートがロックされる前に認識されていない送信元 MAC アドレスを持つ許可されていないコンピュータは、ロックされたポートに接続し、ネットワークに接続することを防止できます。

図 10- 2. Port Security Settings と Table 画面

以下のパラメータを設定できます。

パラメータ	説明
From...To	ポートセキュリティを設定するポートまたはポート範囲を選択します。
Admin State	ポートセキュリティの有効/無効をプルダウンメニューで指定します。Enabled にすると該当ポートは MAC アドレステーブルがロックされます。
Max. Addr. (0-10)	選択したスイッチとポートの MAC アドレス転送テーブルに保存できる MAC アドレス数を指定します。
Lock Addess Mode	プルダウンメニューでスイッチにおけるポートの MAC アドレステーブルのロック動作の方法を指定します。 • *Permanent* – ロックされたアドレスはエージングタイム経過後に削除されません。 • *DeleteOnTimeout* – ロックされたアドレスは、エージングタイム経過後に削除されます。 • *DeleteOnReset* – ロックされたアドレスはリセットされるまで削除されません。

Apply ボタンをクリックし、変更を適用します。

確認: アップリンクポート(DES-3010Gはポート9-10、DES-3018ポートは17-18、DES-3026はポート25-26) はポートセキュリティ機能をサポートしていません。

ポートロックエントリ

ポートセキュリティエントリからエントリを削除するには **Port Lock Entries** 画面を使用します。このポートセキュリティエントリはスイッチが学習して転送データベースに登録したものです。**Security > Port Lock Entries** をクリックし、以下の画面を表示します。

Port Lock Entries Table					
VID	VLAN Name	MAC Address	Port	Type	Delete
1	default	00-08-02-0b-85-d2	2	Permanent	X
1	default	00-08-02-54-10-0a	2	Permanent	X
1	default	00-0c-6e-12-e1-1a	2	Permanent	X
1	default	00-50-8d-36-94-98	2	Permanent	X
1	default	00-50-ba-00-06-03	2	Permanent	X
1	default	00-50-ba-da-00-22	2	Permanent	X
1	default	00-e0-18-72-0d-e6	2	Permanent	X

図 10- 3. Port Lock Entries Table

この機能は **Port Security** 画面の **Mode** で ***Permanent*** か ***DeleteOnReset*** が選択されているときに使用します。別の言い方をするとアドレスが永続的にスイッチに記録されているときしか削除できません。正確な情報により定義されたエントリが画面の中にある場合は対応する MAC アドレスの行の Delete 列の X ボタンをクリックし、削除します。**Next** ボタンをクリックし、エントリリストの次のページを参照します。

この画面では以下の情報を確認できます。

パラメータ	説明
VID	スイッチの転送データベーステーブルに登録されているエントリの VLAN ID です。
VLAN Name	スイッチの転送データベーステーブルに登録されているエントリの VLAN 名です。
MAC Address	スイッチの転送データベーステーブルに登録されているエントリの MAC アドレスです。
Port	MAC アドレスを記録しているポート番号です。
Type	転送データベーステーブルに登録されている MAC アドレスの種類です。Secured_Permanent となっているエントリのみ削除できます。
Delete	X ボタンをクリックすると該当の MAC アドレスが削除されます。

802.1X 認証の設定

802.1X ポートベースと MACベースアクセスコントロール

IEEE 802.1X 規格はクライアントとサーバベースのアクセスコントロールモデルを使用した特定の LAN 上の各種有線/無線デバイスへのアクセスを可能とするためにユーザを認証するセキュリティの規格です。クライアントとサーバ間の EAPOL (Extensible Authentication Protocol over LAN) パケットを中継してネットワークにアクセスするユーザを認証するために RADIUS サーバを使用します。以下の図は基本的な EAPOL パケットを表しています。:

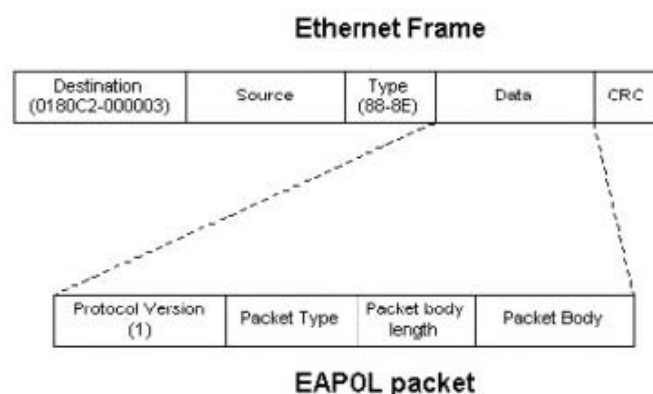



図 10- 4. EAPOL パケット

この方法を使用すると、未認証のデバイスが接続ポート経由で LAN に接続することを制限できます。EAPOL パケットは認証されるまでは指定ポート経由で転送される唯一のトラフィックです。802.1X アクセスコントロール方法は3つの役割を持っており、それぞれがアクセスコントロールセキュリティ方法の作成、状態の保持および動作のために重要です。

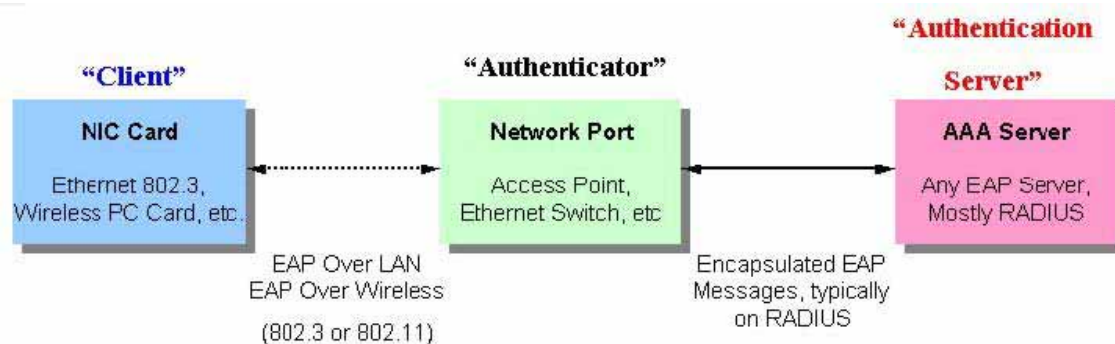



図 10- 5. 802.1X の3つの役割

以下のセクションではより詳しくクライアント、Authenticator および認証サーバの3つの役割について説明します。

認証サーバ

認証サーバはクライアントとAuthenticatorと同じようにネットワークに接続し、RADIUSプログラムを実行し、さらにAuthenticator (スイッチ)に設定されているリモートデバイスです。スイッチポートに接続しているクライアントは、LAN 上のスイッチによって提供されるサービスを受ける前に認証サーバ(RADIUS)により認証される必要があります。認証サーバの役割は EAPOL パケット経由で RADIUS サーバとクライアント間のセキュアな情報を交換することによりネットワークにアクセスしようとするクライアントの一致を証明します。そして、クライアントが LAN および(または)スイッチのサービスへのアクセス許可の有無をスイッチに伝えます。

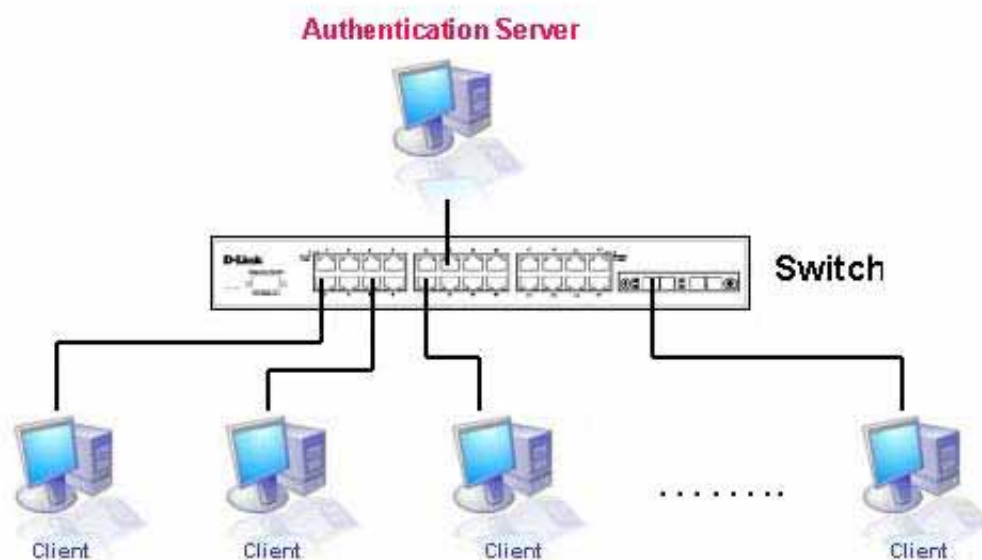



図 10- 6. 認証サーバ

Authenticator

Authenticator (スイッチ) は認証サーバとクライアント間で中継をします。802.1X を使用する場合、Authenticator には2つの目的があります。1つめの目的はアクセスがクライアントに許可される前に Authenticator を通過することが可能な唯一の情報である EAPOL パケットを通じクライアントに認証情報をリクエストすることです。2つめはクライアントから収集した情報を認証サーバで確認し、その後クライアントに情報を戻すことです。

Authenticator を適切に設定するためには以下の3つの手順を行う必要があります。

1. 802.1X を有効にします。
2. 802.1X 設定はポートごとにします。
3. RADIUS サーバをスイッチに設定します。

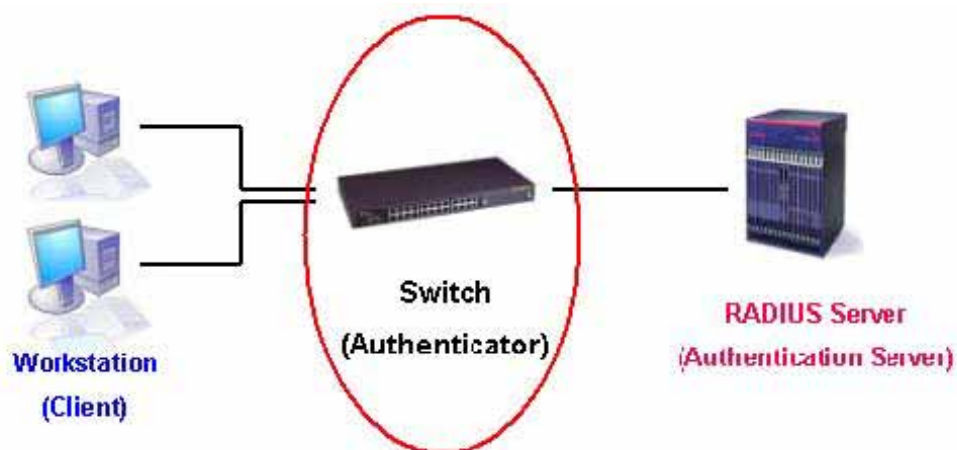



図 10- 7. Authenticator

クライアント

クライアントは簡単に言うとLANまたはスイッチサービスにアクセスを希望するエンドステーションを指します。すべてのエンドステーションには 802.1X プロトコルに準拠したソフトウェアが動作している必要があります。Windows XP にはソフトウェアが含まれています。その他のユーザは 802.1X クライアントソフトウェアを別途用意する必要があります。クライアントは EAPOL パケットを通して LAN またはスイッチへのアクセスリクエストを行い、逆にスイッチからのリクエストにも応答します。

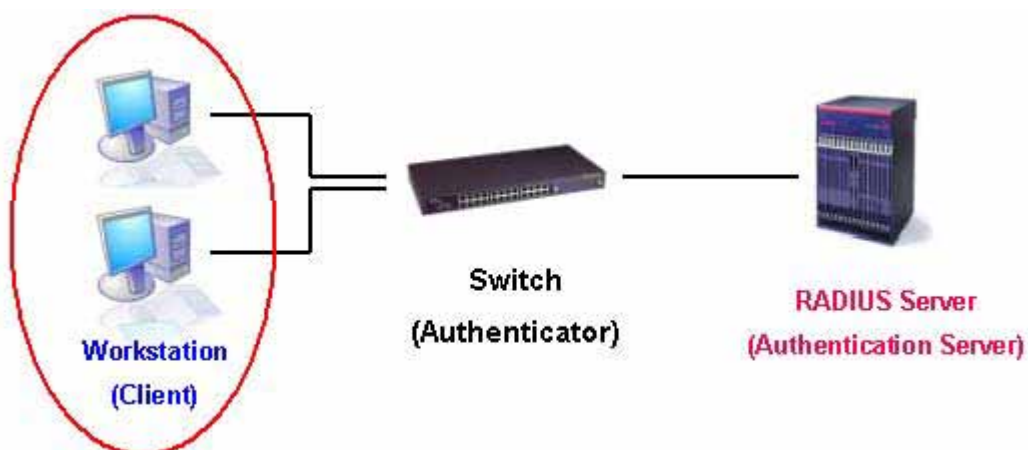



図 10- 8. クライアント

認証プロセス

上記3つの役割を使用している場合、802.1X プロトコルはネットワークへのアクセスを試みるユーザを認証するセキュアな方法を提供します。認証が成功する前に EAPOL パケットだけが通過を許可されます。正しいユーザ名とパスワード(および MAC アドレスにより 802.1X を有効としている場合は MAC アドレス)を持つクライアントがアクセスを許可され、ポートのロックを解除されるまでこのポートはロックされます。一度ロックを解除さると、通常のトラフィックはポートを通過できるようになります。以下の図は認証プロセスが上記3つの役割の状態を完了させる方法についてより詳しく示しています。

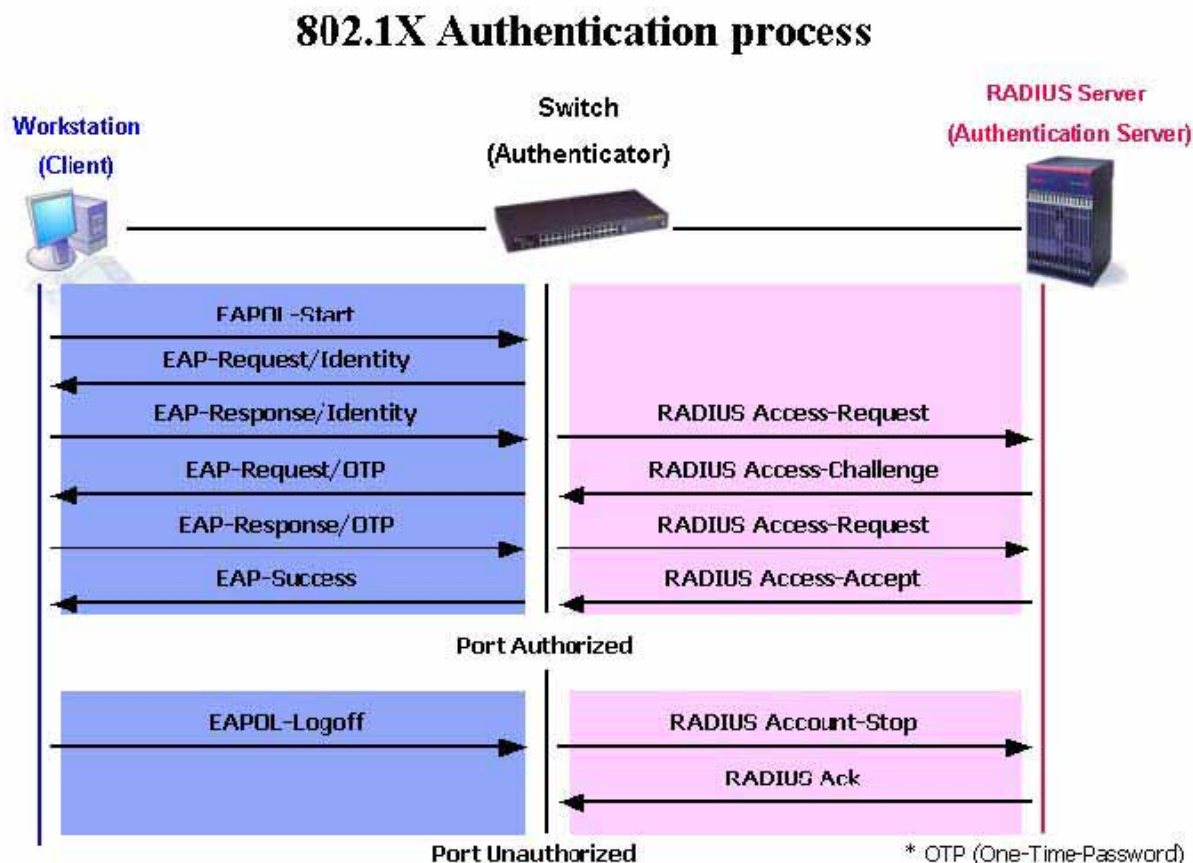



図 10- 9. 802.1X 認証プロセス

D-Link 802.1X ではネットワーク管理者は以下の2つのタイプのアクセスコントロールを選択できます。:

1. ポートベースアクセスコントロール – この方法は1人のユーザだけがリモートの RADIUS サーバによりポートごとに認証されることを要求し、残りのユーザも同じポートをアクセスできるようにします。
2. MAC ベースアクセスコントロール – この方法を使用すると、スイッチは自動的に各ポート 8 個の MAC アドレスを学習してリストに設定します。各 MAC アドレスは、ネットワークへのアクセスを許可される前にリモートの RADIUS サーバを使用してスイッチにより認証される必要があります。

802.1X ポートベースとMACベースネットワークアクセスコントロールについて

802.1X 開発の元々の目的は Point-to-Point LAN の特徴を利用するためでした。インフラストラクチャのようにシングル LAN セグメントが 2 個以上のデバイスを持たない場合、どちらかがブリッジポートとなります。ブリッジポートはリンクのリモートエンドにアクティブなデバイスの接続またはアクティブなデバイスがアクティブでなくなったことを示すイベントを検出します。これらのイベントはポートの認証状態をコントロールし、ポートが認証されない場合に接続デバイスの認証プロセスを初期化するために使用します。これがポートベースネットワークアクセスコントロールです。

ポートベースネットワークアクセスコントロール

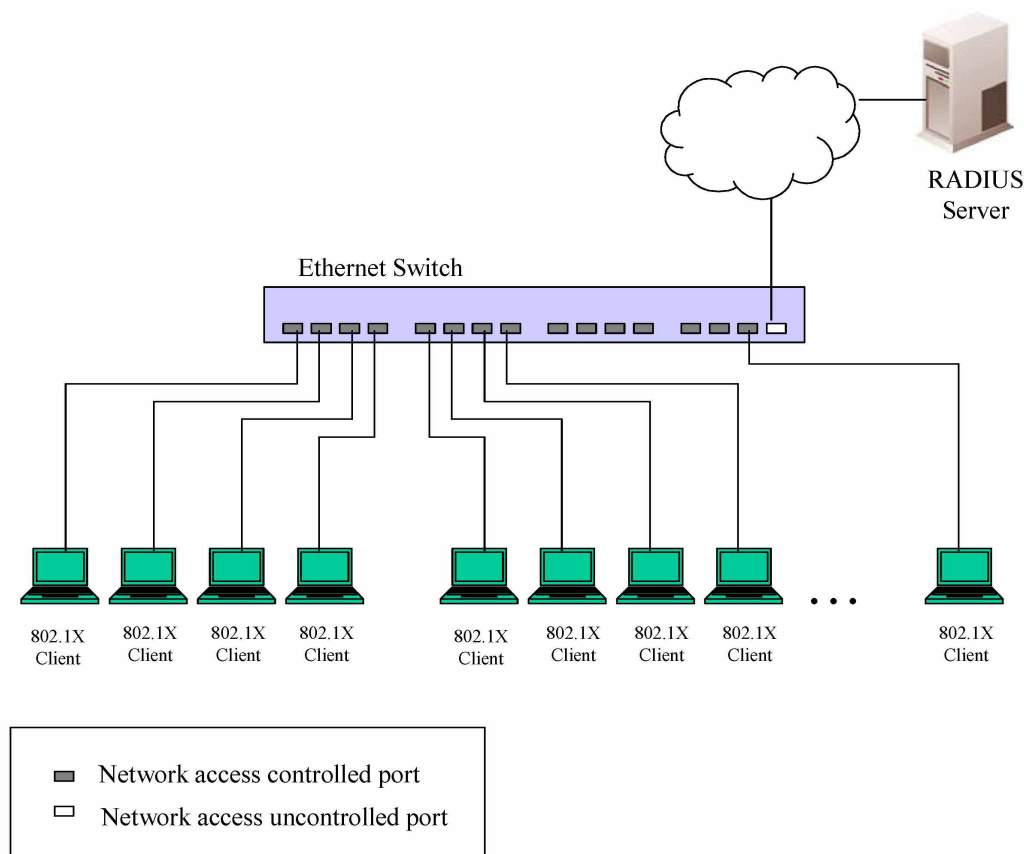



図 10- 10. 代表的なポートベース設定の例

一度接続デバイスが認証に成功すると、その後ポートは認証され、ポートが未認証になるようなイベントが発生するまでポート上のすべてのトラフィックはアクセスコントロール制限にはかかりません。そのためポートは実際に 1 個以上のデバイスが所属する共有 LAN セグメントに接続されている場合、接続デバイスの1つが認証に成功すると共有セグメント上のすべての LAN に対して事実上アクセスを許可することになります。明らかにこの状況で提供されるセキュリティは攻撃に対するガードはゆるい状態になっています。

MAC ベースネットワークアクセスコントロール

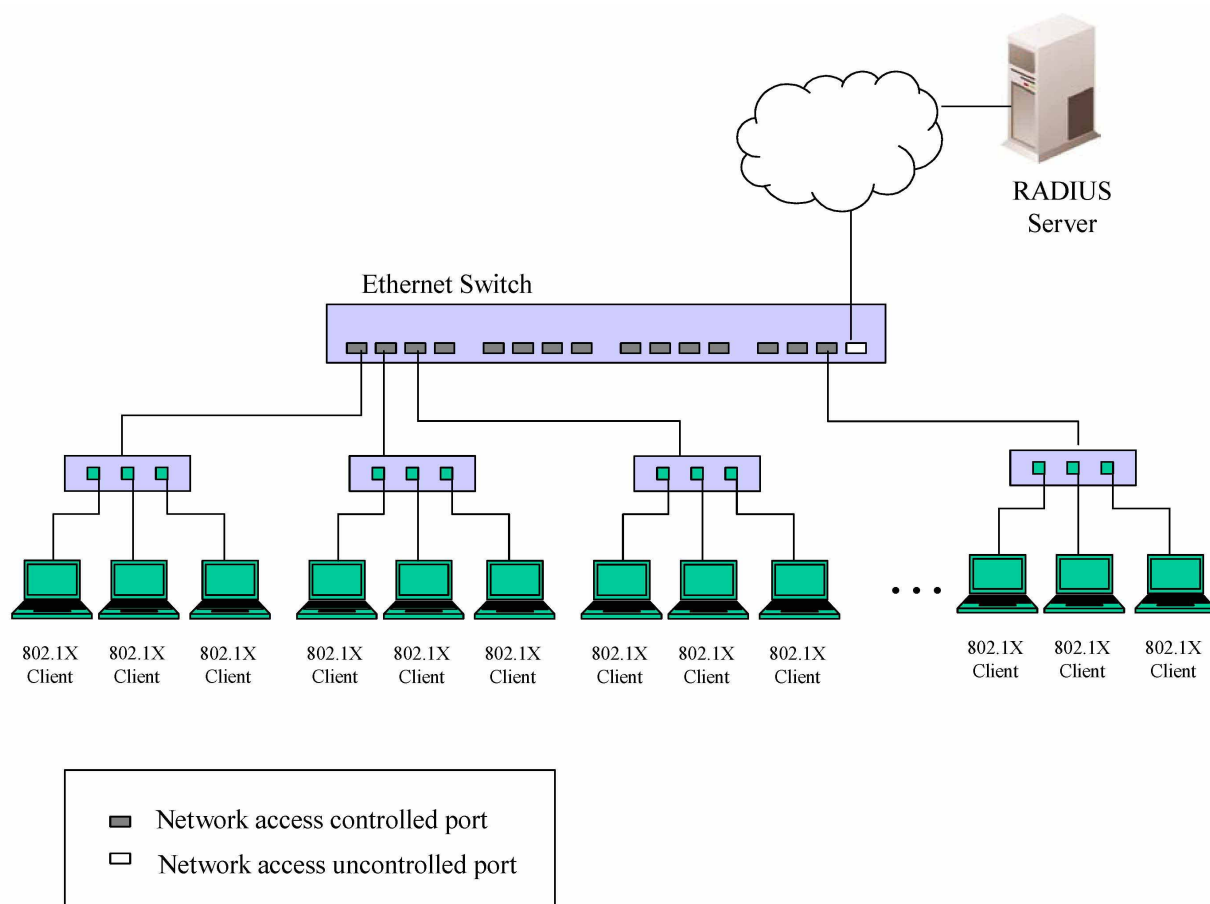



図10- 11. 代表的な MAC ベース設定の例

共有 LAN セグメント内で 802.1X をうまく使用するためには、LAN へのアクセスを希望する各接続デバイスに"logical"(論理)ポートを作成する必要があります。スイッチは 1 個の物理ポートが EAPOL 交換と認証状態の参照の観点から個別に制御される論理ポートにより構成される共有セグメントに接続していると見なします。スイッチは接続している各デバイスの MAC アドレスを学習し、論理ポートを作成します。接続デバイスはこれによりスイッチ経由で LAN と通信ができるようになります。

802.1X Authenticatorの設定

Security > 802.1X > **Configure 802.1X Authenticator Settings**をクリックし、802.1X認証の設定を行います。

802.1X Authenticator Settings

Port	AdmDir	Ctrl Stat	TxPeriod	Quiet Period	Supp-Timeout	Server-Timeout	MaxReq	ReAuth Period	ReAuth Enabled
1	both	auto	30	60	30	30	2	3600	no
2	both	auto	30	60	30	30	2	3600	no
3	both	auto	30	60	30	30	2	3600	no
4	both	auto	30	60	30	30	2	3600	no
5	both	auto	30	60	30	30	2	3600	no
6	both	auto	30	60	30	30	2	3600	no
7	both	auto	30	60	30	30	2	3600	no
8	both	auto	30	60	30	30	2	3600	no
9	both	auto	30	60	30	30	2	3600	no
10	both	auto	30	60	30	30	2	3600	no
11	both	auto	30	60	30	30	2	3600	no
12	both	auto	30	60	30	30	2	3600	no
13	both	auto	30	60	30	30	2	3600	no
14	both	auto	30	60	30	30	2	3600	no
15	both	auto	30	60	30	30	2	3600	no
16	both	auto	30	60	30	30	2	3600	no
17	both	auto	30	60	30	30	2	3600	no
18	both	auto	30	60	30	30	2	3600	no

図 10- 12. 802.1X Authenticator Settings 画面

ポートの設定は対応する**Port**番号のハイパーリンクをクリックし、表示される以下の表を使用します。

802.1X Authenticator Settings

From	Port 1
To	Port 1
AdmDir	both
PortControl	auto
TxPeriod	30
QuietPeriod	60
SuppTimeout	30
ServerTimeout	30
MaxReq	2
ReAuthPeriod	3600
ReAuth	Disabled

Show Authenticators Setting　Apply

図 10- 13. 802.1X Authenticator Settings – Modify 画面

この画面では以下の機能を設定できます。

パラメータ	説明
From … To	設定するポートまたはポート範囲を指定します。
AdmDir	認証の方向を一方向か双方向に指定します。 *in* を選ぶとポートが受信するトラフィックのみ処理します。 *both* を選ぶとポートが受信送信する両方向のトラフィックについて処理します。
PortControl	ポートの認証状態を指定します。 802.1X を無効にするには *forceAuthorized* を選びます。この場合、ポートが認証状態になるのに、どのような認証の交換も必要ありません。つまり、ポートは 802.1X ベースの認証無しのトラフィックを送受信します。 *forceUnauthorized* を選ぶとポートは常に認証されていない状態になり、クライアントからの認証要求を無視します。スイッチはクライアントに対して認証サービスを提供しません。 *auto* を選ぶと 802.1X を有効にし、ポートはまず、認証されていない EAPOL フレームだけを送受信できる状態になります。リンク状態が接続、切断と変化したり、EAPOL-start フレームを受け取ると認証プロセスが始まります。スイッチはクライアントの識別を要求し、クライアントと認証サーバ間の認証メッセージの中継を開始します。 初期値は *auto* です。
TxPeriod	PAE を管理する authenticator の TxPeriod の値を指定します。EAP Request/Identity パケットがクライアントに送信される間隔を決定します。初期値は *30* 秒です。
QuietPeriod	クライアントと認証の交換を失敗した後スイッチが quiet 状態を維持する秒数を指定します。初期値は *60* 秒です。
SuppTimeout	Authenticator とクライアントの通信が切れてタイムアウト状態となる時間を指定します。初期値は *30* 秒です。
ServerTimeout	Authenticator と認証サーバの通信が切れてタイムアウト状態となる時間を指定します。初期値は *30* 秒です。
MaxReq	認証セッションがタイムアウトになるまでに EAP リクエストをクライアントに送信する最大の回数を指定します。初期値は *2* です。
ReAuthPeriod	定期的クライアントの再認証の周期を 0 以外で指定します。初期値は *3600* 秒です。
ReAuth	規則的に最認証を行うかを指定します。初期値は *Disabled* です。

Apply ボタンをクリックし、変更を適用します。ポートごとの **802.1X Authenticator** 設定を確認するには **802.1X Authenticator Settings** テーブルを参照します。

ローカルユーザ

802.1X のローカルユーザ設定を行うためには **Security > 802.1X > Local users** とクリックします。以下の画面でスイッチ上に 802.1X ローカルユーザを設定することができます。

図 10- 14. 802.1X Local User Table Configuration と 802.1X Local User Table 画面

User Name、**Password** および確認用パスワードを入力します。ローカルユーザの設定が完了すると同じ画面に **802.1X Local User Table** が表示されます。

Port Capability

Security > 802.1X > 802.1X Capability Settings をクリックし、以下の画面を表示します。

図 10- 15. 802.1X Capability Settings と Table 画面

スイッチのポートベース認証を設定するためには From/To フィールドでポート範囲を設定します。次に **Capability** のドロップダウンメニューにより選択した Authenticator ごとにポートを有効にします。**Apply** ボタンをクリックし、設定を有効にします。

802.1X capability Settings 画面では以下の設定をします。

パラメータ	説明
From … To	802.1X 設定をするポートまたはポート範囲を指定します。
Capability	2つの役割を選択できます。 *Authenticator* – ユーザはネットワークにアクセスするために認証プロセスを通過する必要があります。 *None* -ポートは 802.1X 機能により制御されません。

ポートベース 802.1X認証におけるポートの初期化

既存の802.1X ポートとMACアドレス設定は、以下の画面で表示および設定をします。

Security > 802.1X > Initialize Port(s) をクリックし、以下の画面を表示します。

Initialize Port

From	To	Apply
Port 1	Port 1	Apply

Initialize Port Table

Port	Auth PAE State	Backend_State	Oper Dir	PortStatus
1	ForceAuth	Success	both	Authorized
2	ForceAuth	Success	both	Authorized
3	ForceAuth	Success	both	Authorized
4	ForceAuth	Success	both	Authorized
5	ForceAuth	Success	both	Authorized
6	ForceAuth	Success	both	Authorized
7	ForceAuth	Success	both	Authorized
8	ForceAuth	Success	both	Authorized
9	ForceAuth	Success	both	Authorized
10	ForceAuth	Success	both	Authorized

図 10- 16. Initialize Port 画面(ポートベース802.1X)

ここではポートまたはポート範囲の初期化を行います。 画面の下部の**Initialize Port Table** はポートの現在のステータスを表示します。

この画面には以下の情報が表示されます。

パラメータ	説明
From … To	初期化するポートを選択します。
Port	スイッチのポートを示す参照用フィールドです。
Auth PAE State	Authenticator PAEの状態を以下のパラメータのいずれかで表示します。: *Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth* または

	ForceUnauth
Backend_State	Backend Authenticationの状態を以下のパラメータのいずれかで表示します。: *Request, Response, Success, Fail, Timeout, Idle* または *Initialize*
Open Dir	使用できる制御方向は *both* と *in* です。
Port Status	コントロールポートのステータスは*Authorized* または *Unauthorized* で表示します。

MACベース 802.1X認証におけるポートの初期化

MAC ベース 802.1X 認証でポートを初期化するためには **Advanced Settings** 画面ではじめに MAC アドレスごとに 802.1X を有効にする必要があります。**Security > 802.1X > 802.1X Initialize Port(s)**とクリックし、以下の画面を表示します。

図 10- 17. Initialize Port(s) (MAC ベース802.1X)

ポートを初期化するためには、はじめに **From** と **To** フィールドでポート範囲を選択してください。それから **MAC Address** フィールドに MAC アドレスを入力し、対応するチェックボックスにチェックを入れます。**Apply** ボタンをクリックし、初期化を開始します。

確認: ポートの初期化の前にスイッチの**Web Management Tool**画面で802.1Xを有効にする必要があります。**Initialize Ports Table**の情報は802.1Xが有効でないと参照できません。

確認: アップリンクモジュールポート(DES-3010Gはポート9-10、DES-3018はポート17-18、DES-3026はポート25-26) は802.1X機能をサポートしていません。

ポートベース 802.1Xにおけるポートの再認証

From と **To** のプルダウンメニューでポートまたはポート範囲を選択し、**Apply** ボタンをクリックすることで再認証を行います。**Apply** をクリックすると **Reauthenticate Port Table** には再認証ポートの現在のステータスが表示されます。

Security > 802.1X > Reauthenticate Port(s) の順でクリックし、以下の画面を表示します。

Reauthenticate Port

From	To	Apply
Port 1	Port 1	Apply

Reauthenticate Port Table

Port	Auth State	BackendState	OperDir	PortStatus
1	ForceAuth	Success	both	Authorized
2	ForceAuth	Success	both	Authorized
3	ForceAuth	Success	both	Authorized
4	ForceAuth	Success	both	Authorized
5	ForceAuth	Success	both	Authorized
6	ForceAuth	Success	both	Authorized
7	ForceAuth	Success	both	Authorized
8	ForceAuth	Success	both	Authorized
9	ForceAuth	Success	both	Authorized
10	ForceAuth	Success	both	Authorized

図 10- 18. Reauthenticate Port と Reauthenticate Port Table 画面

この画面は以下の情報を表示します。

パラメータ	説明
Port	再認証されるポートの番号。
Auth PAE State	Authenticator PAEの状態を次のパラメータのいずれかで表示します。:*Initialize*、*Disconnected*、*Connecting*、*Authenticating*、*Authenticated*、*Aborting*、*Held*、*ForceAuth* または *ForceUnauth*
Backend_State	Backend Authenticationの状態を以下のパラメータのいずれかで表示します。: *Request*、*Response*、*Success*、*Fail*、*Timeout*、*Idle* または *Initialize*
Open Dir	使用できる制御方向は*both*と*in*です。
PortStatus	コントロールポートのステータスは*Authorized* または *Unauthorized*で表示します。

確認: ポートの再認証の前に本スイッチ**Web**トップメニュー画面のSwitch 802.1XをPort_basedにする必要があります。**Reauthenticate Ports Table**の情報は 802.1Xが有効でないと参照できません。

確認: アップリンクモジュールポート(DES-3010Gはポート9-10、DES-3018はポート17-18、DES-3026はポート25-26) は802.1X機能をサポートしていません。

MACベース802.1Xにおけるポートの再認証

MAC ベース 802.1X 認証おけるポート再認証のためには、はじめに **Advanced Settings** 画面で MAC アドレスごとに 802.1X を有効にします。**Security > 802.1X > Reauthenticate Port(s)** をクリックし、以下の画面を表示します。

図 10- 19. Reauthenticate Ports – MAC ベース802.1X

ポートの再認証のためにははじめに **From** と **To** のプルダウンメニューでポートまたはポート範囲を選択します。その後 **MAC Address** フィールドに再認証する MAC アドレスを入力し、チェックボックスにチェックを入れます。**Apply** ボタンをクリックし、再認証を開始します。

確認: ポートの再認証の前に本スイッチ**Web**トップメニュー画面のSwitch 802.1XをMAC_basedにする必要があります。**Reauthenticate Ports Table** の情報は 802.1Xが有効でないと参照できません。

確認: アップリンクモジュールポート(DES-3010Gはポート9-10、DES-3018はポート17-18、DES-3026はポート25-26) は802.1X機能をサポートしていません。

RADIUS サーバ

RADIUS サーバにより集約したユーザ管理やハッカーによるスニファーからの保護が可能になります。Web 管理用には 3 つの画面があります。**Security > 802.1X > RADIUS Server** をクリックし、以下の **Authentic RADIUS Server Setting** 画面を表示します。

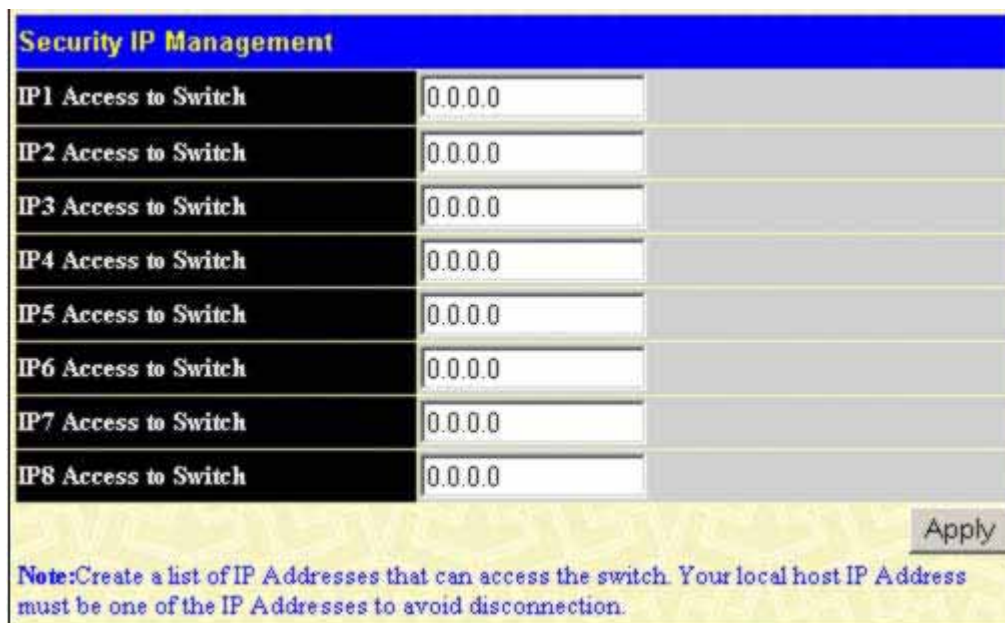



図 10- 20. Authentic RADIUS Server と Current RADIUS Server Settings Table 画面

この画面では以下の情報を確認、設定できます。

パラメータ	説明
Succession	設定する RADIUS サーバを指定します。: *First*、*Second*、*Third*
RADIUS Server	RADIUS サーバの IP アドレスです。
Authentic Port	RADIUS 認証サーバの UDP ポートです。初期値は *1812* です。
Accounting Port	RADIUS アカウントサーバの UDP ポートです。初期値は *1813* です。
Key	RADIUS サーバに設定したものと同一の鍵を指定します。
Confirm Key	RADIUS サーバに設定したものと同一の共有鍵の確認入力をします。
Status	RADIUS サーバの有効(*Valid*)、無効(*Invalid*)を設定します。

トラストホスト

Security > Trusted Host とクリックし、以下の画面を表示します。

図 10- 21. Security IP Management メニュー

Security IP Management を使用してリモートステーションがスイッチの管理を行うことを許可します。指定された 1 個以上の管理ステーションを定義するために選択すると、IPアドレスによって定義された選択ステーションだけが Web マネージャまたは Telnet セッション経由で管理する権利を持つことができます。管理ステーションの IP 設定を定義するためには IP アドレスを入力し、**Apply** ボタンをクリックします。

トラフィックセグメンテーション

トラフィックセグメンテーションは 1 つのポートからシングルスイッチ(スタンドアロンモード) 上のポートグループまたはスイッチスタック内の別のスイッチのポートグループへのトラフィックの流れを制限するのに使用します。この方法によるトラフィックの流れの分割は VLAN による制限に似ていますが、もっと限定的なものです。マスタースイッチ CPU のオーバーヘッドを増加させないでトラフィックを直接操作します。

Security > Traffic Segmentation とクリックし、以下の画面を表示します。

Port	Configuration	Setup
Port 1	View	Setup

Current Traffic Segmentation Table

Port	Port Map
1	1-18
2	1-18
3	1-18
4	1-18
5	1-18
6	1-18
7	1-18
8	1-18
9	1-18
10	1-18
11	1-18
12	1-18
13	1-18
14	1-18
15	1-18
16	1-18
17	1-18
18	1-18

図 10- 22. Current Traffic Segmentation Table

Setup ボタンをクリックし、以下の **Setup Forwarding ports** 画面を表示します。

図 10- 23. Setup Forwarding ports 画面

この画面ではスイッチスタック内で決められたスイッチ上のどのポートが他のポートにパケットを転送するかを決定することができます。

トラフィックセグメンテーションの設定は 2 段階に分かれます。まず、スイッチのポートを **Port** プルダウンメニューで選択し、次にスイッチと最初に指定したポートからパケットを受け取ることができるポートを指定します。

Apply ボタンをクリックすると送信ポートと受信可能なポートの組み合わせが **Traffic Segmentation Table** に表示されます。

Port のドロップダウンメニューでパケットを送信するスイッチのポートを選択します。

Forward Port チェックボックスによりパケットを転送できるスイッチのポートを選択します。これらのポートは上で指定したポートからのパケットを受信することができます。

Apply ボタンをクリックし、**Traffic Segmentation Table** 内に設定を入力します。

セクション 11

モニタリング

CPU 使用率

CPU Utilization は CPU が使用している割合を一定間隔で平均を計算し表示します。**Monitoring > CPU Utilization** をクリックし、**CPU Utilization** 画面を参照します。

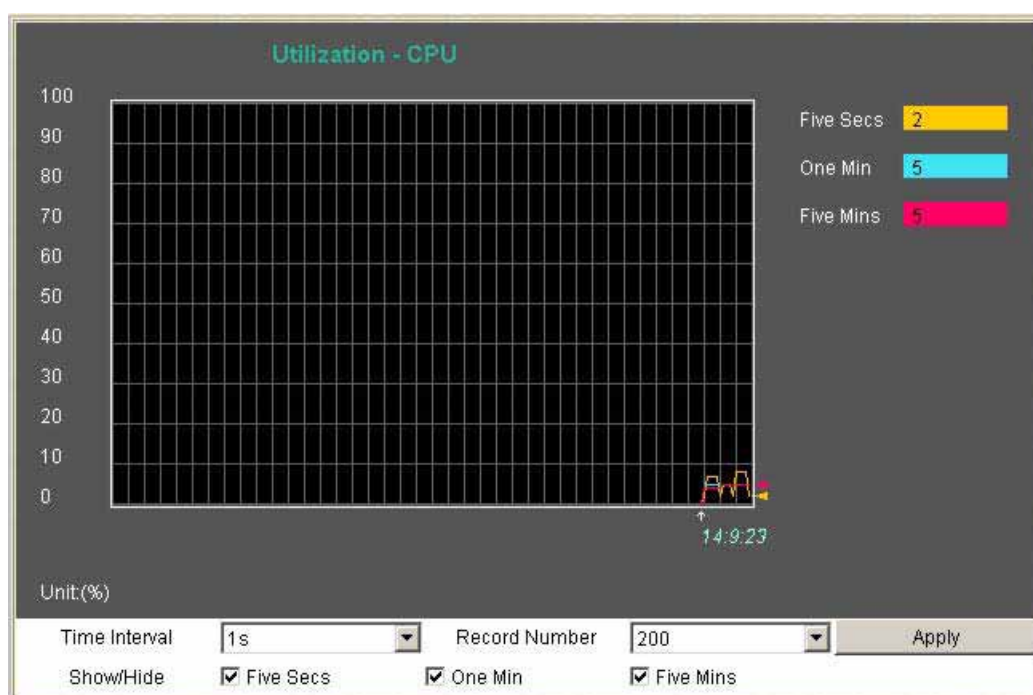



図 11- 1. CPU Utilization グラフ

Web画面の上部にあるスイッチのリアルタイムグラフィックを使用し、ポートをクリックしてポートごとのCPU使用率を参照します。参照用パラメータを入力後、**Apply** ボタンをクリックし、設定を適用します。画面は自動的にリフレッシュし新しく更新した統計情報を表示します。

以下の参照用パラメータを設定できます。

パラメータ	説明
Time Interval *[1s]*	*1s* ～ *60s*(s は秒)を選択します。初期値は *1s*(1 秒)です。
Record Number *[200]*	スイッチがポーリングする回数を *20*～*200* で選択します。初期値は *200* です。
Utilization	CPU 使用率の表示/非表示のチェックをします。

ポート使用率

Port Utilization はポート上で使用可能な帯域の合計を割合で表示します。

Monitoring > Port Utilization をクリックし、ポート使用率を参照します。

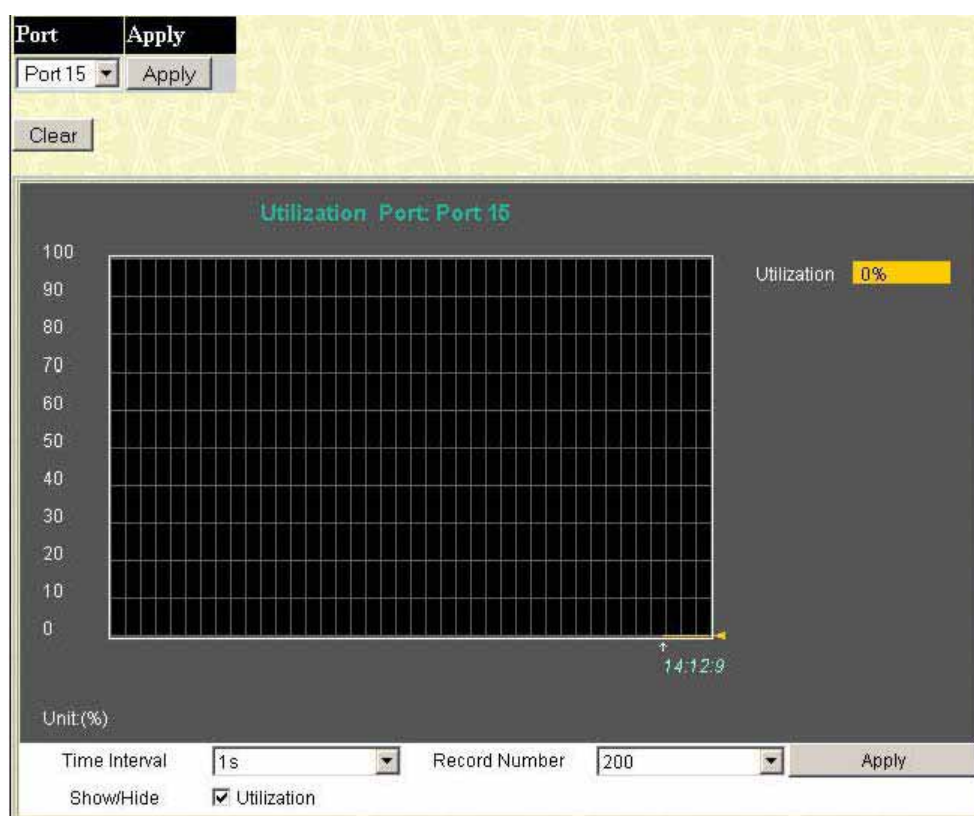



図 11- 2. Port Utilization 画面

Web 画面の上部にあるスイッチのリアルタイムグラフィックを使用し、ポートをクリックしてポートごとの統計情報を参照します。以下のフィールドを設定することができます。

パラメータ	説明
Time Interval	*1s* ～ *60s*(s は秒)を選択します。初期値は *1s*(1 秒)です。
Record Number	スイッチがポーリングする回数を *20*～*200* で選択します。初期値は *200* です。

Clear をクリックし、グラフをリフレッシュします。**Apply** ボタンをクリックし、設定を適用します。

パケット統計情報

Web ブラウザ上で各種パケット統計情報の折れ線または表を参照できます。6 個の画面が表示されます。

受信パケット(RX)

Monitoring メニューの **Packets** フォルダの **Received (RX)** をクリックし、以下のスイッチの受信パケットのグラフを参照します。**Port** のプルダウンメニューでポートを選択し、統計情報を参照します。Web ページの上部にあるスイッチのリアルタイムグラフィックでポートをクリックすることもできます。

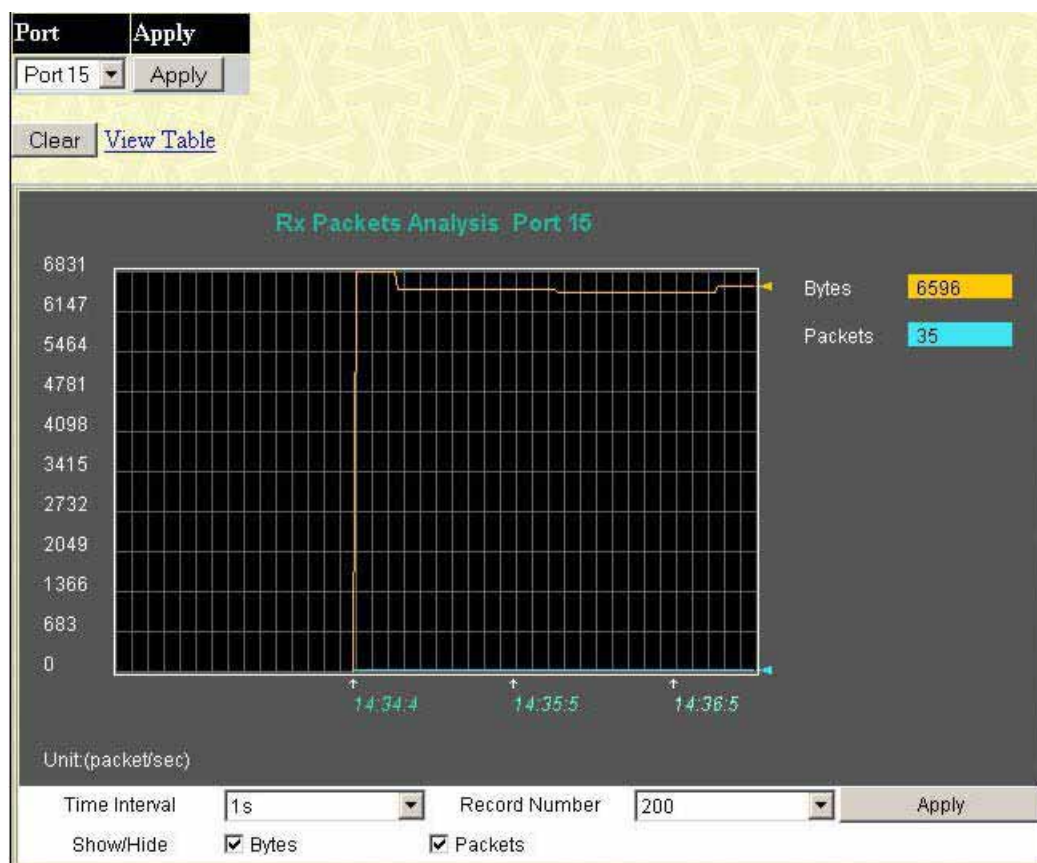



図 11- 3. Rx パケット分析画面(バイトとパケットの折れ線グラフ)

Received Packets Table を参照するためには View Table をクリックします。以下の表が表示されます。

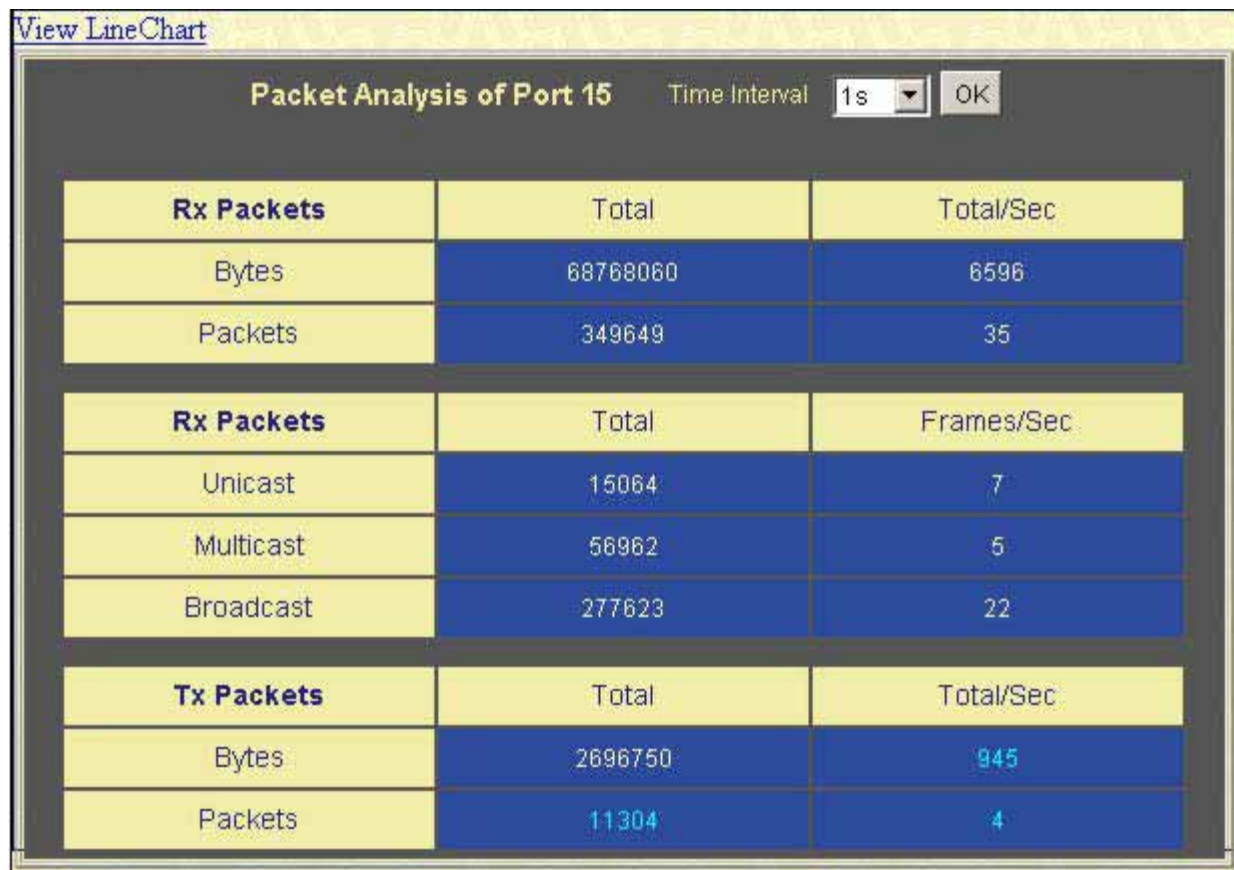



図 11- 4. Rx パケット分析テーブル

以下のフィールドを設定または参照できます。

パラメータ	説明
Time Interval [1s]	*1s* ～ *60s*(sは秒)を選択します。初期値は*1s*(1秒)です。
Record Number [200]	スイッチがポーリングする回数を*20*～*200*で選択します。初期値は*200*です。
Bytes	ポートが受信したバイト数をカウントします。
Packets	ポートが受信したパケット数をカウントします。
Unicast	ユニキャストアドレスが受信した有効なパケットの合計数をカウントします。
Multicast	マルチキャストアドレスが受信した有効なパケットの合計数をカウントします。
Broadcast	ブロードキャストアドレスが受信した有効なパケットの合計数をカウントします。
Show/Hide	バイト数とパケット数を表示するかどうかをチェックします。
Clear	このボタンをクリックし、この画面のすべての統計情報をクリアします。
View Table	このボタンをクリックし、折れ線グラフ表示からテーブル表示にします。
View Line Chart	このボタンをクリックし、テーブル表示から折れ線グラフ表示にします。

UMB Cast (RX)

Monitoring > Packets > UMB Cast (RX) とクリックし、スイッチが受信する UMB cast パケットを参照します。**Port** プルダウンメニューを使用し、統計情報を参照するポートを選択します。Web ページの上部にあるスイッチのリアルタイムグラフィックでポートをクリックすることもできます。

図 11- 5. パケット分析画面 (ユニキャスト、マルチキャスト、およびブロードキャストパケットの折れ線グラフ)

UMB Cast Tableを参照するためには<u>View Table</u> リンクをクリックします。以下の画面が表示されます。

View Line Chart

Packet Analysis of Port 15 Time Interval 1s OK

Rx Packets	Total	Total/Sec
Bytes	69560952	6625
Packets	353674	34

Rx Packets	Total	Frames/Sec
Unicast	15921	6
Multicast	57544	5
Broadcast	280209	21

Tx Packets	Total	Total/Sec
Bytes	2856203	1065
Packets	11967	5

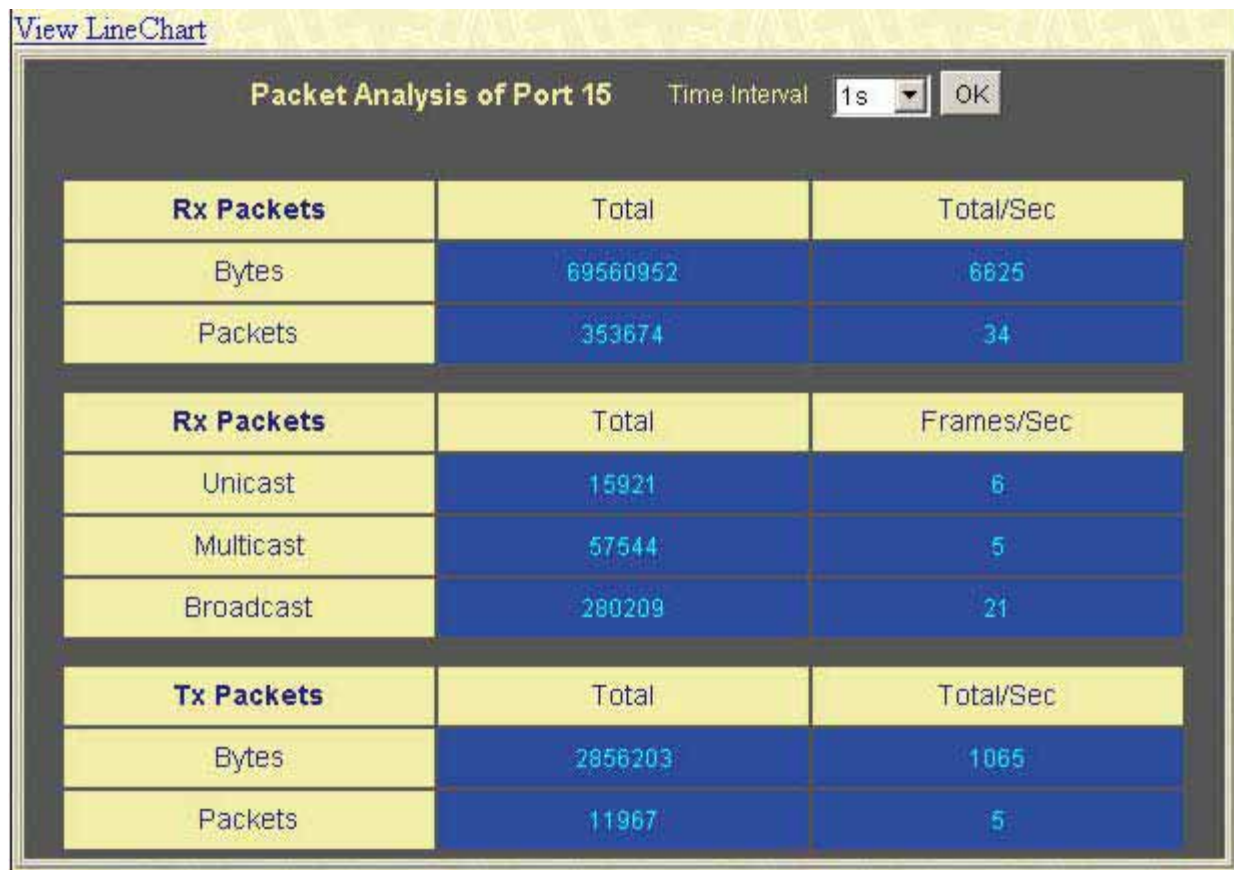



図 11- 6. Rx パケット分析 画面(ユニキャスト、マルチキャスト、およびブロードキャストパケットのテーブル)

以下のフィールドを設定または参照できます。

パラメータ	説明
Time Interval [1s]	*1s* ～ *60s*(sは秒)を選択します。初期値は*1s*(1秒)です。
Record Number [200]	スイッチがポーリングする回数を*20*～*200*で選択します。初期値は*200*です。
Unicast	ユニキャストアドレスが受信した有効なパケットの合計数をカウントします。
Multicast	マルチキャストアドレスが受信した有効なパケットの合計数をカウントします。
Broadcast	ブロードキャストアドレスが受信した有効なパケットの合計数をカウントします。
Show/Hide	マルチキャスト、ブロードキャスト、およびユニキャストを表示するかどうかをチェックします。
Clear	このボタンをクリックし、この画面のすべての統計情報をクリアします。
View Table	このボタンをクリックし、折れ線グラフ表示からテーブル表示にします。
View Line Chart	このボタンをクリックし、テーブル表示から折れ線グラフ表示にします。

転送 (TX)

Monitoring メニューの **Packets** フォルダ内の **Transmitted (TX)**リンクをクリックし、以下のスイッチから転送されるグラフを参照します。**Port** プルダウンメニューを使用し、統計情報を参照するポートを選択します。Web ページの上部にあるスイッチのリアルタイムグラフィックでポートをクリックすることもできます。

図 11- 7. Tx パケット分析画面 (バイトとパケットの折れ線グラフ)

Transmitted (TX) Tableを参照するためには View Tableをクリックします。以下の画面が表示されます。

View LineChart		
Packet Analysis of Port 15 Time Interval 1s OK		
Rx Packets	Total	Total/Sec
Bytes	3695371	6372
Packets	17471	32
Rx Packets	Total	Frames/Sec
Unicast	1864	5
Multicast	2951	4
Broadcast	12656	20
Tx Packets	Total	Total/Sec
Bytes	1173500	1891
Packets	1785	6

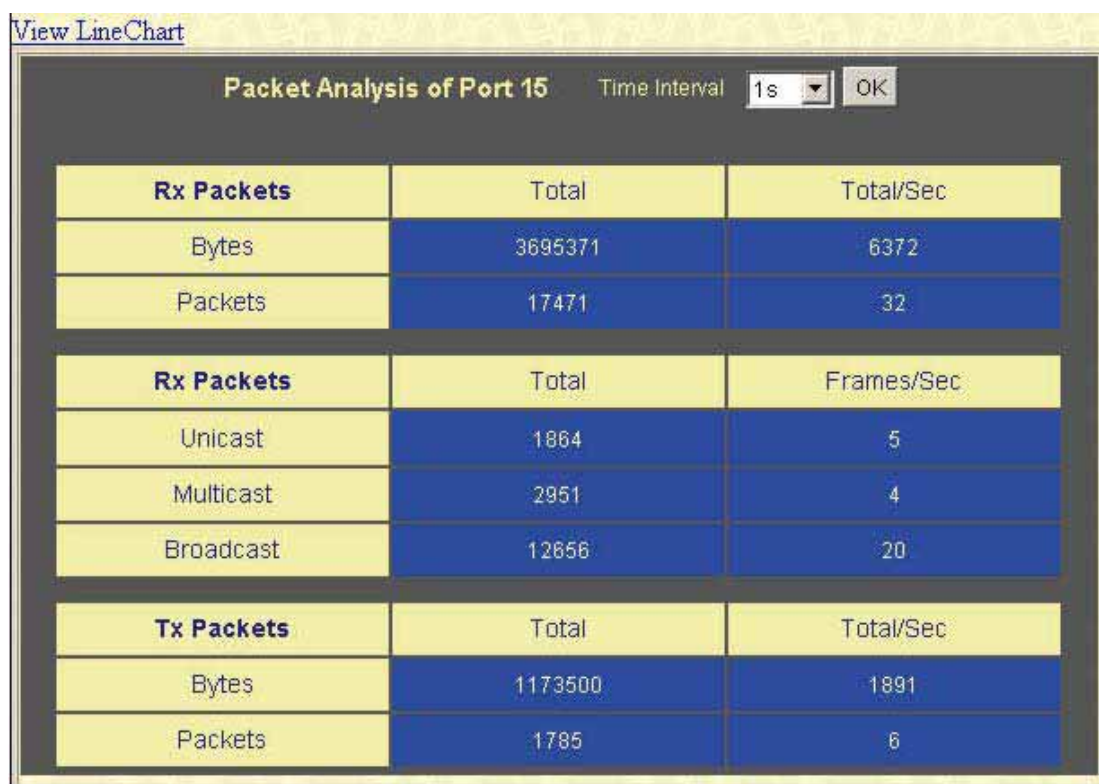



図 11- 8. Tx パケット分析画面 (バイトとパケットのテーブル)

以下のフィールドを設定、または参照できます。

パラメータ	説明
Time Interval [1s]	*1s* ～ *60s*(sは秒)を選択します。初期値は*1s*(1秒)です。
Record Number [200]	スイッチがポーリングする回数を*20*～*200*で選択します。初期値は*200*です。
Bytes	ポートから正常に受信したバイト数をカウントします。
Packets	ポートから正常に受信したパケット数をカウントします。
Unicast	ユニキャストアドレスが送信した有効なパケットの合計数をカウントします。
Multicast	マルチキャストアドレスが送信した有効なパケットの合計数をカウントします。
Broadcast	ブロードキャストアドレスが送信した有効なパケットの合計数をカウントします。
Show/Hide	バイト数とパケット数を表示するかどうかをチェックします。
Clear	このボタンをクリックし、この画面のすべての統計情報をクリアします。
View Table	このボタンをクリックし、折れ線グラフ表示からテーブル表示にします。
View Line Chart	このボタンをクリックし、テーブル表示から折れ線グラフ表示にします。

パケットエラー

Webブラウザによりスイッチ管理エージェントにより収集されるポートエラーの統計情報を折れ線グラフまたは表で表示します。4個の画面があります。

受信 (RX)

Monitoring メニューの **Packet Errors** フォルダの **Received (RX)** をクリックし、以下のようなスイッチが受信したエラーパケットのグラフを参照します。**Port** プルダウンメニューを使用し、統計情報を参照するポートを選択します。Web ページの上部にあるスイッチのリアルタイムグラフィックでポートをクリックすることもできます。

図11- 9. Rx エラー分析画面 (折れ線グラフ)

Received Error Packets Table を参照するためには View Table をクリックします。以下の画面が表示されます。

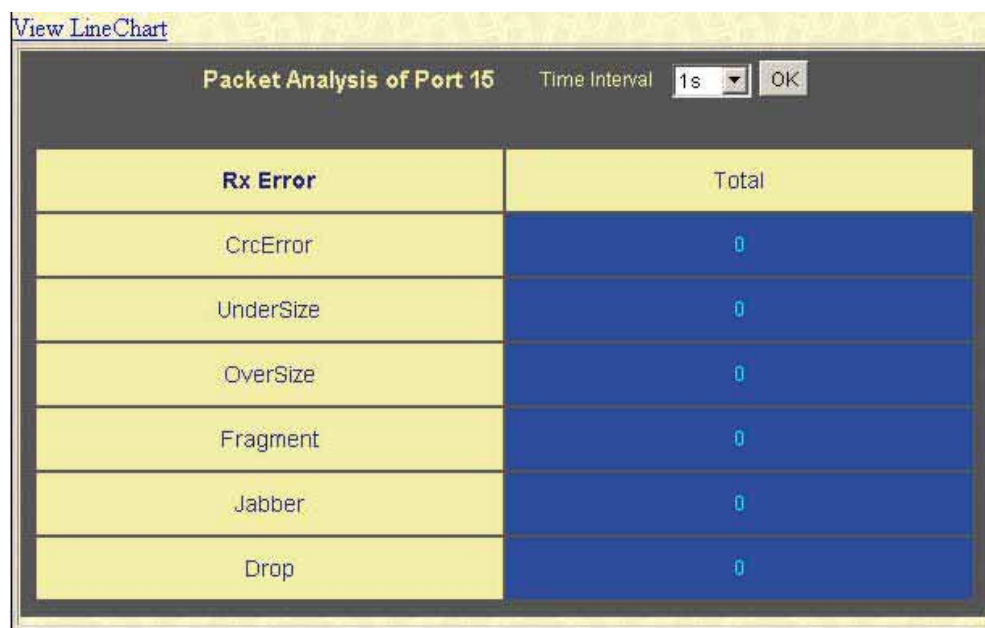



図 11- 10. Rx エラー分析画面 (テーブル)

以下のフィールドを設定、または参照できます。

パラメータ	説明
Time Interval [1s]	*1s* ～ *60s*(sは秒)を選択します。初期値は*1s*(1秒)です。
Record Number [200]	スイッチがポーリングする回数を*20*～*200*で選択します。初期値は*200*です。
CrcError	CRCエラーになったパケット数をカウントします。
UnderSize	許可されている最小パケットサイズ(64バイト)よりも小さいが、CRCチェックで問題がないことを検出されたパケットの数。このアンダーサイズパケットは通常、コリジョンフラグメントやノーマルネットワークであることを示しています。
OverSize	1518オクテットより長い受信パケット数、または、VLANフレームが1522オクテットである場合、MAX_PKT_LEN(1522) より大きい受信パケット数をカウントします。
Fragment	不正なフレーム、または無効なCRCのいずれかを持つ64バイト未満のパケット数。通常コリジョンにより生じます。
Jabber	MAX_PKT_LEN(1522)バイトより長いパケットの数。
Drop	スイッチを再起動してからポートが破棄したパケット数。
Show/Hide	CrcError、UnderSize、OverSize、Fragment、Jabber、およびDrop errorsを表示するかどうかをチェックします。
Clear	このボタンをクリックし、この画面のすべての統計情報をクリアします。
View Table	このボタンをクリックし、折れ線グラフ表示からテーブル表示にします。
View Line Chart	このボタンをクリックし、テーブル表示から折れ線グラフ表示にします。

転送 (TX)

Monitoring メニューの **Packet Errors** フォルダの **Transmitted(TX)** をクリックし、以下のようなスイッチが受信したエラーパケットのグラフを参照します。**Port** プルダウンメニューを使用し、統計情報を参照するポートを選択します。Web ページの上部にあるスイッチのリアルタイムグラフィックでポートをクリックすることもできます。

図 11- 11. Tx エラー分析(折れ線グラフ)

Transmitted Error Packets Tableを参照するためには View Tableをクリックします。以下の画面が表示されます。

Tx Error	Total
ExDefer	0
LateColl	0
ExColl	0
SingColl	0
Coll	0
CRCError	0

図 11- 12. Tx エラー分析(テーブル)

以下のフィールドを設定、または参照できます。

パラメータ	説明
Time Interval *[1s]*	*1s* ～ *60s*(sは秒)を選択します。初期値は*1s*(1秒)です。
Record Number *[200]*	スイッチがポーリングする回数を*20*～*200*で選択します。初期値は*200*です。
ExDefer	特定のインタフェースへの最初の送信が回線ビジーのために遅延したパケット数をカウントします。
CRC Error	CRCエラーになったパケット数をカウントします。
LateColl	パケットの送信に512bit timesより大きい往復遅延時間を検出されたコリジョンの回数をカウントします。
ExColl	Excessive Collisionのために送信エラーをとなったパケット数。
SingColl	Single Collision Frames。1個以上のコリジョンにより送信されていなかったパケットで送信に成功したした数。
Coll	このネットワークセグメントでのコリジョン合計数の概算。
Show/Hide	ExDefer、LateColl、ExColl、SingColl、およびColl errorsを表示するかどうかをチェックします。
Clear	このボタンをクリックし、この画面のすべての統計情報をクリアします。
View Table	このボタンをクリックし、折れ線グラフ表示からテーブル表示にします。
View Line Chart	このボタンをクリックし、テーブル表示から折れ線グラフ表示にします。

パケットサイズ

Monitoring メニューの **Packet Size** をクリックし、以下の画面を表示します。Web マネージャはスイッチが受信したパケットを 6 個のグループに整理し、サイズによってクラス分けして折れ線グラフまたは表にします。2つの画面が提供されます。**Port** プルダウンメニューを使用し、統計情報を参照するポートを選択します。Web ページの上部にあるスイッチのリアルタイムグラフィックでポートをクリックすることもできます。

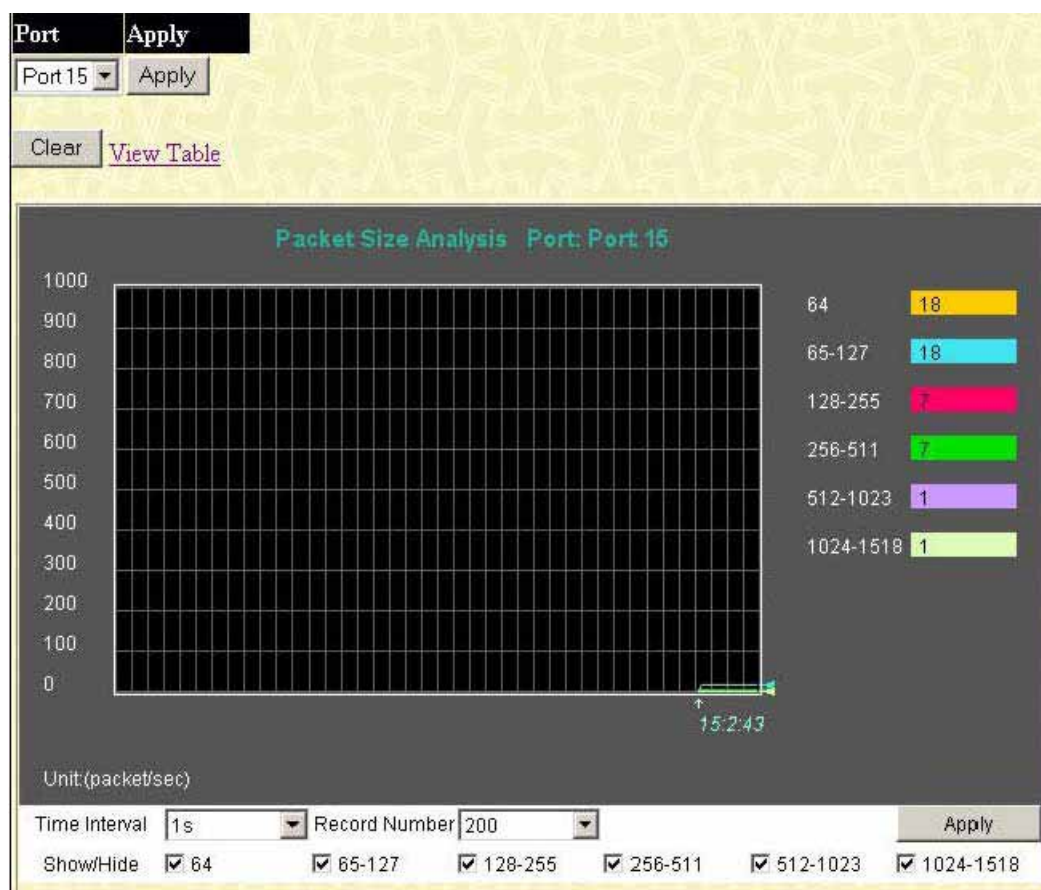



図 11- 13. Rx サイズ分析画面 (折れ線グラフ)

Packet Size Analysis Tableを参照するためには<u>View Table</u>をクリックします。

図 11- 14. Rx サイズ分析画面 (テーブル)

以下のフィールドを設定または参照できます。

パラメータ	説明
Time Interval [1s]	*1s* ～ *60s*(sは秒)を選択します。初期値は*1s*(1秒)です。
Record Number [200]	スイッチがポーリングする回数を*20*～*200*で選択します。初期値は*200*です。
64	(FCSオクテットを含むフレームを除く)長さが64オクテットの(不正なパケットを含む)パケット数の合計。
65-127	(FCSオクテットを含むフレームを除く)長さが65～127オクテットの(不正なパケットを含む)パケット数の合計。
128-255	(FCSオクテットを含むフレームを除く)長さが128～255オクテットの(不正なパケットを含む)パケット数の合計。
256-511	(FCSオクテットを含むフレームを除く)長さが256～511オクテットの(不正なパケットを含む)パケット数の合計。
512-1023	(FCSオクテットを含むフレームを除く)長さが512～1023オクテットの(不正なパケットを含む)パケット数の合計。
1024-1518	(FCSオクテットを含むフレームを除く)長さが1024～1518オクテットの(不正なパケットを含む)パケット数の合計。
Show/Hide	64、65-127、128-255、256-511、512-1023、または 1024-1518 の受信パケットを表示するかどうかをチェックします。
Clear	このボタンをクリックし、この画面のすべての統計情報をクリアします。
View Table	このボタンをクリックし、折れ線グラフ表示からテーブル表示にします。
View Line Chart	このボタンをクリックし、テーブル表示から折れ線グラフ表示にします。

MAC アドレステーブル

スイッチのダイナミックMAC アドレスフォワーディングテーブルを参照できます。スイッチはMAC アドレスとポート番号間の連携を学習し、フォワーディングテーブル内にエントリを作成します。これらのエントリはスイッチ経由でパケットを転送するために使用されます。

MAC Address Forwarding Tableを参照するためには**Monitoring**メニューから**MAC Address**をクリックします。

VID	Vlan Name	MAC Address	Port	Type
1	default	00-00-00-48-49-88	15	Dynamic
1	default	00-00-01-02-03-a2	15	Dynamic
1	default	00-00-11-22-33-45	15	Dynamic
1	default	00-00-50-77-16-00	15	Dynamic
1	default	00-00-5e-00-01-5f	15	Dynamic
1	default	00-00-e2-2f-44-ec	15	Dynamic
1	default	00-00-e2-64-e3-3e	15	Dynamic
1	default	00-00-e2-93-66-06	15	Dynamic
1	default	00-00-e2-98-fd-cd	15	Dynamic
1	default	00-01-02-03-92-27	15	Dynamic
1	default	00-01-06-30-10-63	15	Dynamic
1	default	00-01-30-12-13-02	15	Dynamic
1	default	00-01-6c-b7-ce-17	15	Dynamic
1	default	00-02-06-12-34-56	15	Dynamic
1	default	00-02-3f-72-c4-eb	15	Dynamic
1	default	00-02-a5-fd-66-97	15	Dynamic
1	default	00-02-b3-a5-a9-19	15	Dynamic
1	default	00-03-09-18-10-01	15	Dynamic
1	default	00-03-44-ae-bc-12	15	Dynamic
1	default	00-03-47-91-4a-1c	15	Dynamic

図 11- 15. MAC Address Table

次のパラメータをMACアドレステーブル内で使用できます。

パラメータ	説明
VLAN Name	フォワーディングテーブルを表示するために VLAN 名を入力します。
MAC Address	フォワーディングテーブルを表示するために MAC アドレスを入力します。
Port	プルダウンメニューを使用してポートを選択します。
Find	ユーザが定義したポート、VLAN または MAC アドレスに対応するデータベースを検索し、表示します。
VID	ポートが所属する VLAN の VLAN ID
MAC Address	アドレステーブルに入力した MAC アドレス
Port	上記 MAC アドレスに対応するポート
Type	スイッチが MAC アドレスを取得した方法。*Dynamic*、*Self*、*Static* and Static.
Next	アドレステーブルの次ページに移ります。
View All Entry	アドレステーブルのすべてのエントリを参照します。
Delete All Entry	アドレステーブルのすべてのエントリを削除します。

スイッチヒストリログ

スイッチの管理エージェントによって編集されるスイッチのヒストリログを表示します。**Monitoring**フォルダをオープンし、 **Switch History Log**クリックします。

Switch History

Sequence	Time	Log Text
21	0000/00/00 00:11:45	Console session timed out (Username: Anonymous, IP:0.0.0.0, MAC:00-00-00-00-00-00)
20	0000/00/00 00:02:08	Successful login through Web (Username: Anonymous, IP:10.53.13.94, MAC:00-50-8D-36-94-98)
19	0000/00/00 00:01:41	Successful login through Console (Username: Anonymous, IP:0.0.0.0, MAC:00-00-00-00-00-00)
18	0000/00/00 00:00:06	Port 2 link up, 100Mbps FULL duplex
17	0000/00/00 00:00:05	System started up
16	0000/00/00 00:01:51	Firmware upgraded successfully (Username: Anonymous, IP:0.0.0.0, MAC:00-00-00-00-00-00)
15	0000/00/00 00:01:37	Firmware upgrade was unsuccessful! (Username: Anonymous, IP:0.0.0.0, MAC:00-00-00-00-00-00)
14	0000/00/00 00:00:28	Successful login through Console (Username: Anonymous, IP:0.0.0.0, MAC:00-00-00-00-00-00)
13	0000/00/00 00:00:06	Port 2 link up, 100Mbps FULL duplex
12	0000/00/00 00:00:05	System started up
11	0000/00/00 00:13:14	Firmware upgraded successfully (Username: Anonymous, IP:0.0.0.0, MAC:00-00-00-00-00-00)
10	0000/00/00 00:12:54	Firmware upgrade was unsuccessful! (Username: Anonymous, IP:0.0.0.0, MAC:00-00-00-00-00-00)
9	0000/00/00 00:11:40	Successful login through Console (Username: Anonymous, IP:0.0.0.0, MAC:00-00-00-00-00-00)
8	0000/00/00 00:00:10	Port 2 link up, 100Mbps FULL duplex
7	0000/00/00 00:00:05	System started up
6	0000/00/00 00:10:27	Configuration saved to flash (Username: Anonymous, IP:0.0.0.0, MAC:00-00-00-00-00-00)
5	0000/00/00 00:08:00	Configuration saved to flash (Username: Anonymous, IP:0.0.0.0, MAC:00-00-00-00-00-00)
4	0000/00/00 00:00:47	Successful login through Console (Username: Anonymous, IP:0.0.0.0, MAC:00-00-00-00-00-00)
3	0000/00/00 00:00:06	Port 1 link up, 100Mbps FULL duplex
2	0000/00/00 00:00:05	System started up

Clear Next

図 11- 16. Switch History Log 画面

スイッチはログ内に SNMP トラップを受信するステーション、およびコンソール接続している PC に対するイベント情報を記録できます。**Next** をクリックし、**Switch History Log** の次ページに移動します。**Clear** をクリックすると **Switch History Log** をクリアします。

以下の情報が表示されます。

パラメータ	説明
Sequence	スイッチのヒストリログへのエントリが作成されるときに加算されるカウンタ。最後のエントリ(もっとも高い数字の Sequence)を上に表示します。
Time	スイッチが最後に起動してからのスイッチのイベント発生日時を表示します。
Log Text	ヒストリログエントリを発生させたイベントに関する説明を表示します。

ログ設定

Use the **Log Settings** メニューを使用してスイッチログの保存のために使用するスケジュールまたは項目を定義します。

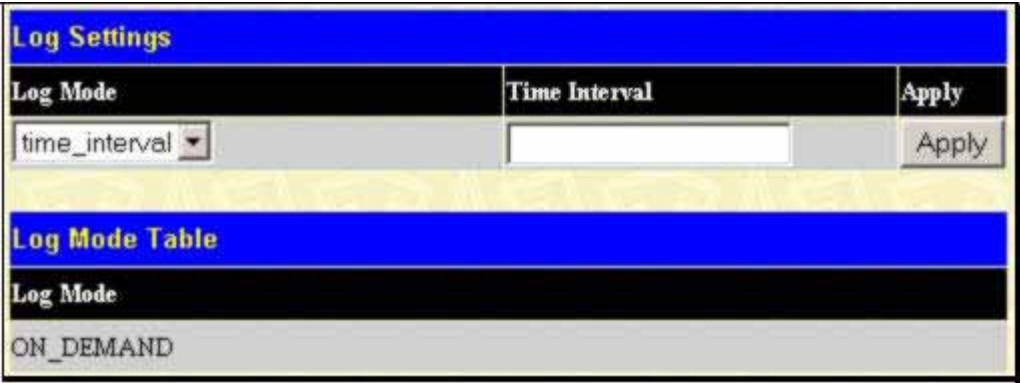



図 11- 17. Log Settings メニュー

Log Mode を選択し、**Apply** ボタンをクリックして設定を適用します。

パラメータ	説明
time_interval	保存する最小間隔(秒)を指定します。
on_demand	ログを受信するホストによりリクエストされた場合にログが保存されます。
log_trigger	前もって設定したトリガーがログを Syslog ホストに保存するよう要求した場合にログは保存されます。config syslog host コマンドを使用してトリガーの種類を決定します。

IGMP Snooping グループ

この画面でスイッチの **IGMP Snooping Group Table** を参照します。IGMP Snooping 機能によってスイッチを通過する IGMP パケットからマルチキャストグループ IP アドレスと対応する MAC アドレスを読み取ることができます。検索された IGMP レポート数は **Reports** フィールドに表示されます。

IGMP Snooping Group Tableを参照するためには**Monitoring** メニューの **IGMP Snooping Group** をクリックします。

図 11- 18. IGMP Snooping Group Table

左上に VID を入力し、**Search** をクリックし、VID ごとの **IGMP Snooping Group Table** を検索できます。

以下のパラメータを参照することができます。

パラメータ	説明
VLAN ID	マルチキャストグループの VLANID
Multicast Group	マルチキャストグループの IP アドレス
MAC Address	マルチキャストグループの MAC アドレス
Reports	このグループに受信したレポートの合計数
Port Map	IGMP パケットが検索されるポートを表示します。

確認:スイッチの IGMP snooping を設定するために **L2 Features** フォルダで **IGMP Snooping** を選択します。IGMP snooping に関連する設定と情報についてはこのマニュアルのセクション 7 の **IGMP Snooping** を参照してください。

ルータポートの表示

スイッチの各ポートが現在ルータポートとして設定されているかを表示します。コンソールまたは Web ブラウザで設定されたルータポートはスタティックルータポートとして **S** で表示されます。スイッチにダイナミックに設定されたルータポートは **D** と表示されます。

Total Entries:2

Browse Router Port

VLAN ID	VLAN Name
1	default

Ports

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

Next

図11- 19. Browse Router Port 画面

ARP テーブルの表示

Browse ARP Table 画面は **Monitoring** フォルダで **Brows ARP Table** メニューをクリックし、表示します。この画面ではスイッチ上の現在の ARP エントリを表示します。**ARP Table** をクリアする場合は、**Clear All** をクリックします。

Clear All

Browse ARP Table

Interface Name	IP Address	MAC Address	Type
System	10.0.0.0	ff-ff-ff-ff-ff-ff	Local/Broadcast
System	10.17.11.11	00-80-c8-92-2d-58	Dynamic
System	10.53.13.33	00-40-05-00-30-01	Local
System	10.53.13.94	00-50-8d-36-94-98	Dynamic
System	10.255.255.255	ff-ff-ff-ff-ff-ff	Local/Broadcast

図 11- 20. Browse ARP Table 画面

セッションテーブル

Current Session Table はスイッチの現在の設定セッションの詳細情報を表示します。ユーザのセッション **ID**、初期の **Login Time**、**Live Time**、**From**(スイッチへの接続方法)、**Level** およびユーザの **Name** などの情報が表示されます。この画面を最新の情報に更新するためには **Reload** ボタンをクリックします。

Reload

Total Entries :1

Current Session Table

ID	Login Time	Live Time	From	Level	Name
8	00000 days 00:00:04	00:31:49.890	Serial Port	1	Anonymous

図 11- 21. Current Session Table

ポートアクセスコントロール情報

以下の画面でポートスイッチのポートごとに 802.1X 統計情報をモニターします。**Port Access Control** 画面を参照するためには **Monitoring** フォルダを開き、**Port Access Control** フォルダをクリックします。モニターのために 6 個の画面があります。

確認：このセクション内の **Authenticator State**, **Authenticator Statistics**, **Authenticator Session Statistics** および **Authenticator Diagnostics** 画面を参照するためには 802.1X 設定がポートまたは MAC アドレスによって有効になっている必要があります。Web ブラウザ設定メニュートップの Device Information 画面の **Switch 802.1X** エントリで Port_based または MAC_based を選択し、802.1X を有効にします。

RADIUS認証

この表は RADIUS 認証プロトコルのクライアント側の RADIUS 認証クライアントの動作に関連する情報を表示します。クライアントが暗号鍵を共有している RADIUS 認証サーバごとに列があります。**RADIUS Authentication** を参照するためには **Monitoring > Port Access Control > RADIUS Authentication** をクリックします。

ServerIndex	InvalidServer	Identifier	ServerIPAddr	UDP Port	Timeouts	Requests	Challenges	Accepts	Rejects	RoundTripTime
1	0	DES-3010G	0.0.0.0	0	0	0	0	0	0	0
2	0	DES-3010G	0.0.0.0	0	0	0	0	0	0	0
3	0	DES-3010G	0.0.0.0	0	0	0	0	0	0	0

図 11- 22. RADIUS Authentication 画面

統計情報の更新間隔を *1s* から *60*s (s：秒)で選択します。初期値は *1s*(1 秒)です。現在の統計情報をクリアするためには左上角の *Clear* ボタンをクリックします。

以下の情報が表示されます。

パラメータ	説明
Server Index	クライアントが暗号鍵を共有している各 RADIUS 認証サーバに割り当てられた識別子の番号。
InvalidServer	認証サーバに登録されていないクライアントからのアカウンティング要求の回数。
Identifier	製品名を表示します。
UDP Port	クライアントがこのサーバにリクエストを送信するために使用する UDP ポート。
Timeouts	本サーバへの認証タイムアウト数。タイムアウトの後、クライアントは同じサーバにリトライするか、異なるサーバに送信するか、または送信を終了します。同じサーバへのリトライはタイムアウトと同様に再転送としてカウントされます。異なるユーザへの送信はタイムアウトと同様に Request としてカウントされます。
Requests	サーバに送信された RADIUS アクセス要求パケット数。再送信は含まれません。
Challenges	本サーバより受信した RADIUS Access-Challenge パケット数(有効/無効パケット)。

Accepts	本サーバから受信した RADIUS アクセス許可パケット数(有効/無効パケット)。
Rejects	本サーバより受信した RADIUS アクセス拒否パケット数(有効/無効パケット)。
RoundTripTime	もっとも最近 RADIUS 認証サーバから送信されたアクセスリプライ/アクセスチャレンジ とアクセス要求の間隔(1/100 秒単位)。
AccessRetrans	本 RADIUS 認証サーバに再送信された RADIUS アクセス要求パケット数。
PendingRequests	まだタイムアウトになっていない、もしくはレスポンスを受信していないこのサーバ行きの RADIUS Access -Request パケット数。この変数は Access-Request が送信された時に 1 つ増加し、Access-Accept、Access-Reject または Access-Challenge の受信、タイムアウトまたは再転送時に1つ減少します。
AccessResponses	本サーバより受信した不正な形式の RADIUS Access-Response パケット数。不正形式のパケットには不正な長さのパケットも含まれます。不正認証、署名属性、または不明なタイプは不正なアクセス responses としては含まれません。
BadAuthenticators	本サーバより受信した不正認証や署名属性 RADIUS Access-Response パケット数。
UnknownTypes	本サーバから認証 ポートに受信した不明なタイプの RADIUS パケット数。
PacketsDropped	本サーバから認証ポートに受信し、何らかの理由で破棄した RADIUS パケット数。

RADIUS Accounting

本画面では RADIUS Accounting クライアントを管理するために使用する管理オブジェクトとそれらに関連した現在の統計情報を表示します。クライアントが暗号鍵を共有している RADIUS 認証サーバごとに列があります。**RADIUS Accounting** を参照するために **Monitoring > Port Access Control > RADIUS Accounting** をクリックします。

図 11- 23. RADIUS Accounting 画面

統計情報を更新するためには更新間隔を *1s* ～ *60s* (s は秒)から指定します。初期値は *1* 秒です。現在の統計情報をクリアするためには左上の *Clear* ボタンをクリックします。

以下の情報が表示されます。

パラメータ	説明
Server IP Add	クライアントが暗号鍵を共有する RADIUS Accounting サーバの IP アドレス
ServerIndex	認証サーバの番号
InvalidServerAddr	認証サーバに登録されていないクライアントからのアカウンティング要求の回数
Identifier	製品名を表示します。
Server Port Number	クライアントがこのサーバにリクエストを送信するために使用している UDP ポート
Timeouts	このサーバへの accounting タイムアウト数。タイムアウトの後、クライアントは同じサーバにリトライするか、異なるサーバに送信するか、または送信を終了します。同じサーバへのリトライはタイムアウトと同様に再転送としてカウントされます。異なるユーザへの送信はタイムアウトと同様に Accounting-Request としてカウントされます。
Requests	送信された RADIUS Accounting-Request パケット数。これは再転送のパケット数は含まれていません。
Responses	Accounting ポートで受信したサーバからの RADIUS パケット数
RoundTripTime	RADIUS accounting サーバからクライアントに送信されるもっとも新しい Accounting-Response と Accounting-Request の間隔。
AccessRetrans	この RADIUS accounting サーバに転送された RADIUS Access-Request パケット数。
PendingRequests	まだタイムアウトになっていない、もしくはレスポンスを受信していないサーバ行きの RADIUS Accounting-Request パケット数。この変数は Accounting-Request が送信された時に 1 つ加算し、Accounting-Response の受信、タイムアウトまたは再転送時に1つ減少します。
MalformedResponses	このサーバから Accounting ポートに受信した不正な形式の RADIUS Accounting-Response パケット数。Malformed packets には不正な長さのパケットを含まれます。認証エラーや不明なタイプは不正な accounting responses としては含まれません。
BadAuthenticators	このサーバから Accounting ポートに受信した不正な認証を含む RADIUS Accounting-Response パケット数
UnknownTypes	このサーバから Accounting ポートに受信した不明なタイプの RADIUS パケット数。
PacketsDropped	このサーバから accounting ポートに受信し、何らかの理由で破棄した RADIUS パケット数 。

Authenticator 診断

この表には各ポートに関連する Authenticator の操作に関する診断情報が含まれます。Authenticator 機能をサポートする各ポートの表にエントリが表示されます。**Authenticator Diagnostics** を参照するためには、**Monitoring > Port Access Control > Auth Diagnostics** の順にクリックします。

Port	EntersConnecting	EapLogoffsConnecting	EntersAuthenticating	SuccessAuthenticating	TimeoutsAuthenticating	FailAuthenticating	ReauthsAuthenticating	EapStartsAuthenticating	EapLogoffAuthenticating	ReauthsAuthenticated	EapStartsAuth
1	-	-	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-	-	-

図 11- 24. Authenticator Diagnostics 画面

統計情報を更新するためには更新間隔を *1s* ～ *60s* (s は秒)から指定します。初期値は *1* 秒です。現在の統計情報をクリアするためには左上の *Clear* ボタンをクリックします。

以下の情報が表示されます。

パラメータ	説明
Port	システムによってポートに割り当てられた識別番号。
EntersConnecting	他の状態から CONNECTING 状態に状態遷移した回数をカウントします。
EapLogoffsConnecting	EAPOL-Logoff メッセージを受信した結果、CONNECTING から DISCONNECTED に状態遷移した回数をカウントします。
EntersAuthenticating	サプリカントから EAP-Response/Identity メッセージを受信した結果、CONNECTING から AUTHENTICATING に状態遷移した回数をカウントします。
SuccessAuthenticating	Backend Authentication 状態が Supplicant の認証成功(authSuccess = TRUE)となった結果、AUTHENTICATING から AUTHENTICATED に状態遷移した回数をカウントします。
TimeoutsAuthenticating	Backend Authentication 状態が認証のタイムアウト(authTimeout = TRUE)となった結果、AUTHENTICATING から ABORTING に状態遷移した回数をカウントします。
FailAuthenticating	Backend Authentication 状態が認証失敗(authFail = TRUE)となった結果、AUTHENTICATING から HELD に状態遷移した回数をカウントします。
ReauthsAuthenticating	再認証リクエスト (reAuthenticate = TRUE)の結果、AUTHENTICATING から ABORTING に状態遷移した回数をカウントします。
EapStartsAuthenticating	サプリカントから EAPOL-Start メッセージを受信した結果、AUTHENTICATING から ABORTING に状態遷移した回数をカウントします。
EapLogoffAuthenticating	サプリカントから EAPOL-Logoff メッセージを受信した結果、AUTHENTICATING から ABORTING に状態遷移した回数をカウントします。
ReauthsAuthenticated	再認証リクエスト (reAuthenticate = TRUE)の結果、AUTHENTICATED から CONNECTING に状態遷移した回数をカウントします。
EapStartsAuthenticated	サプリカントから EAPOL- Start メッセージを受信した結果、AUTHENTICATED から CONNECTING に状態遷移した回数をカウントします。
EapLogOffAuthenticated	サプリカントから EAPOL-Logoff メッセージを受信した結果、AUTHENTICATED から DISCONNECTED に状態遷移した回数をカウントします。

Responses	State Machine が認証サーバに Initial Access-Request パケットを送信した(すなわちエントリ上の sendRespToServer が RESPONSE 状態となった)回数をカウントします。Authenticator が認証サーバとの通信を試みることを意味します。
AccessChallenges	State Machine が認証サーバから Initial Access-Challenge パケットを受信した(すなわち aReq が TRUE となり RESPONSE 状態を終了した)回数をカウントします。認証サーバが Authenticator との通信をしていることを意味します。
OtherRequestToSupplicant	State Machine が EAP-Request パケット(Identity、Notification、Failure、または Success メッセージではない)をサプリカントに送信する(すなわちエントリ上の txReq が REQUEST 状態となった)回数をカウントします。Authenticator が EAP-method を選択したことを意味します。
ResponsesFromSupplicant	State Machine が Initial EAP-Request に対してパケットサプリカントからのレスポンスを受信し、そのレスポンスが EAP-NAK より他のものであった(すなわち rxResp が TRUE となり State Machine は REQUEST から RESPONSE 状態になったがそのレスポンスは EAP-NAK ではない)回数をカウントします。サプリカントが Authenticator の選択した EAP-method に応答することができることを意味します。
AuthSuccesses	State Machine が認証サーバから Accept メッセージを受信した(すなわち aSuccess が TRUE となり RESPONSE から SUCCESS に状態遷移した)回数をカウントします。サプリカントが認証サーバでの認証に成功したことを意味します。
AuthFails	State Machine が認証サーバから Reject メッセージを受信した(すなわち aFail が TRUE となり RESPONSE から FAIL に状態遷移した)回数をカウントします。サプリカントが認証サーバでの認証に失敗したことを意味します。

Authenticator セッション統計情報

この表には各ポートに関連する Authenticator PAE に関するセッションオブジェクト統計情報が含まれます。Authenticator 機能をサポートする各ポートの表にエントリが表示されます。**Authenticator Session Statistics** を参照するためには、**Monitoring > Port Access Control > AuthSession Statistics** の順にクリックします。

Authenticator Session Counter of Unit 1 Time Interval 1s OK

Port	Frames Rx	Frames Tx	UserName	Time	Terminate Cause	Octets Rx	Octets Tx	ID	Authentic Method
1	0	0		0	SupplicantLogoff	0	0		Remote Authentication Server
2	0	0		0	SupplicantLogoff	0	0		Remote Authentication Server
3	0	0		0	SupplicantLogoff	0	0		Remote Authentication Server
4	0	0		0	SupplicantLogoff	0	0		Remote Authentication Server
5	0	0		0	SupplicantLogoff	0	0		Remote Authentication Server
6	0	0		0	SupplicantLogoff	0	0		Remote Authentication Server
7	0	0		0	SupplicantLogoff	0	0		Remote Authentication Server
8	0	0		0	SupplicantLogoff	0	0		Remote Authentication Server
9	0	0		0	SupplicantLogoff	0	0		Remote Authentication Server
10	0	0		0	SupplicantLogoff	0	0		Remote Authentication Server
11	0	0		0	SupplicantLogoff	0	0		Remote Authentication Server
12	0	0		0	SupplicantLogoff	0	0		Remote Authentication Server
13	0	0		0	SupplicantLogoff	0	0		Remote Authentication Server
14	0	0		0	SupplicantLogoff	0	0		Remote Authentication Server
15	0	0		0	SupplicantLogoff	0	0		Remote Authentication Server
16	0	0		0	SupplicantLogoff	0	0		Remote Authentication Server
17	0	0		0	SupplicantLogoff	0	0		Remote Authentication Server
18	0	0		0	SupplicantLogoff	0	0		Remote Authentication Server

図 11- 25. Authenticator Session Counter 画面

統計情報を更新するためには更新間隔を *1s* ～ *60s* (s は秒)から指定します。初期値は *1* 秒です。現在の統計情報をクリアするためには左上の *Clear* ボタンをクリックします。

以下の情報が表示されます。

パラメータ	説明
Port	システムによってポートに割り当てられた識別番号。
Frames Rx	このポートがセッション中に受信したユーザデータフレーム数。
Frames Tx	このポートがセッション中に転送したユーザデータフレーム数。
UserName	Supplicant PAE との一致を表すユーザ名。
Time	セッション時間(秒)。
Terminate Cause	セッションが終了した原因。以下の 8 個の原因があります。 1) Supplicant ログオフ 2) ポートのエラー 3) Supplicant 再起動 4) 再認証の失敗 5) AuthControlledPortControl が ForceUnauthorized に設定された。 6) ポートの再初期化 7) ポート管理が無効 8) まだ終了していない

Octets Rx	このポートがセッション中に受信したオクテット数。
Octets Tx	このポートがセッション中に転送したオクテット数。
ID	セッションの識別子。(半角英数字 3 文字以上)。
Authentic Method	セッションを確立するために使用する認証方式。有効な方式は以下のとおりです。 (1) Remote Authentic Server – 認証サーバが Authenticator のシステムより外部にある。 (2) Local Authentic Server -認証サーバが Authenticator のシステム内にある。

Authenticator 統計情報

この表には各ポートに関連する Authenticator PAE に関する統計情報オブジェクトが含まれます。Authenticator 機能をサポートする各ポートの表にエントリが表示されます。**Authenticator Statistics** を参照するためには、**Monitoring > Port Access Control > Auth Statistics** の順にクリックします。

図 11- 26. Authenticator Statistics 画面

統計情報を更新するためには更新間隔を *1s* ～ *60s* (s は秒)から指定します。初期値は *1* 秒です。現在の統計情報をクリアするためには左上の *Clear* ボタンをクリックします。

以下の情報が表示されます。

パラメータ	説明
Port	システムによってポートに割り当てられた識別番号。
Frames Rx	Authenticator が受信した有効な EAPOL フレーム数。
Frames Tx	Authenticator が送信した EAPOL フレーム数。
Start Rx	Authenticator が受信した EAPOL Start フレーム数。
ReqId Tx	Authenticator が送信した EAP Req/Id フレーム数。

LogOff Rx	Authenticator が受信した EAPOL Logoff フレーム数。
Req Tx	Authenticator が送信した EAP Request フレーム数。
Rx RespId	Authenticator が受信した EAP Resp/Id フレーム数。
Resp Rx	Authenticator が受信した有効な EAP Response フレーム(Resp/Id フレーム以外)数。
Invalid Rx	Authenticator が受信した認識されないフレームタイプを含む EAPOL フレーム数。
Error Rx	Authenticator が受信した Packet Body Length が不正な EAPOL フレーム数。
Last Version	受信 EAPOL フレームをもっとも最近送信したプロトコルバージョン。
Last Source	受信 EAPOL フレームをもっとも最近送信した送信元 MAC アドレス。

Authenticator State

本セクションではスイッチの 802.1X ステータスを説明します。Authenticator State を参照するためには、**Monitoring > Port Access Control > Auth State** の順にクリックします。

Port	Auth_PAE_State	Backend_State	PortStatus
1	ForceAuth	Success	Authorized
2	ForceAuth	Success	Authorized
3	ForceAuth	Success	Authorized
4	ForceAuth	Success	Authorized
5	ForceAuth	Success	Authorized
6	ForceAuth	Success	Authorized
7	ForceAuth	Success	Authorized
8	ForceAuth	Success	Authorized
9	ForceAuth	Success	Authorized
10	ForceAuth	Success	Authorized
11	ForceAuth	Success	Authorized
12	ForceAuth	Success	Authorized
13	ForceAuth	Success	Authorized
14	ForceAuth	Success	Authorized
15	ForceAuth	Success	Authorized
16	ForceAuth	Success	Authorized
17	ForceAuth	Success	Authorized
18	ForceAuth	Success	Authorized

図 11- 27. Authenticator State 画面 – ポートベース802.1X

図11- 28. Authenticator State 画面 – MAC ベース802.1X

本画面は選択デバイスの各ポートの **Authenticator State** を表示します。本画面を更新するためには更新間隔を *1s* ～ *60s* (s は秒)から指定し、**OK** ボタンをクリックします。初期値は *1* 秒です。

以下の情報が表示されます。

パラメータ	説明
MAC Address	Authenticator の MAC アドレスを表示します。
Auth PAE State	**Authenticator PAE State** は次のとおりです。: *Initialize*、*Disconnected*、*Connecting*、*Authenticating*、*Authenticated*、*Aborting*、*Held*、*Force_Auth* または *Force_Unauth*
Backend State	**Backend Authentication State** は次のとおりです。: *Request*、*Response*、*Success*、*Fail*、*Timeout*、*Idle* または *Initializa*
Port Status	制御ポートのステータス: *Authorized* または *Unauthorized*

リセット

スイッチをリセットする時の **Reset** 機能にはいくつかのオプションがあります。現在の設定の一部は残りますが、その他の設定は出荷時設定に戻ります。

確認: Reset System オプションだけは出荷時設定を NV-RAM に書き込み、スイッチを再起動します。他のすべてのオプションは現在の設定を出荷時設定に戻しますが、この設定は保存されません。**Reset System** はスイッチの設定を工場出荷状態まで戻します。

図 11- 29. Factory Reset to Default Value 画面

システムの再起動

以下のメニューでスイッチを再起動します。

図 11- 30. Reboot System 画面

Yes をチェックするとスイッチは再起動する前に現在の設定を NV-RAM に保存します。

No をチェックするとスイッチは再起動する前に現在の設定を保存しません。すべての設定情報は破棄され、最後に保存した時の設定が使われます。

Restart ボタンをクリックするとスイッチは再起動します。

変更の保存

本スイッチは通常の RAM と NV-RAM(不揮発 RAM)の 2 レベルのメモリを内蔵しています。いくつかの設定は反映するために再起動が必要です。スイッチを再起動すると RAM 内部の設定は消去され、NV-RAM に保存された設定が読み込まれます。そのため、再起動する前にはすべての設定を NV-RAM に保存する必要があります。

Save Changes には次の3つのオプションがあります。

- **Save Config** ー現在の設定をNV-RAMに保存します。この設定は再起動時にロードされます。
- **Save Log** ーヒストリログを保存します。
- **Save All** ー設定ファイルとログファイルを保存します。

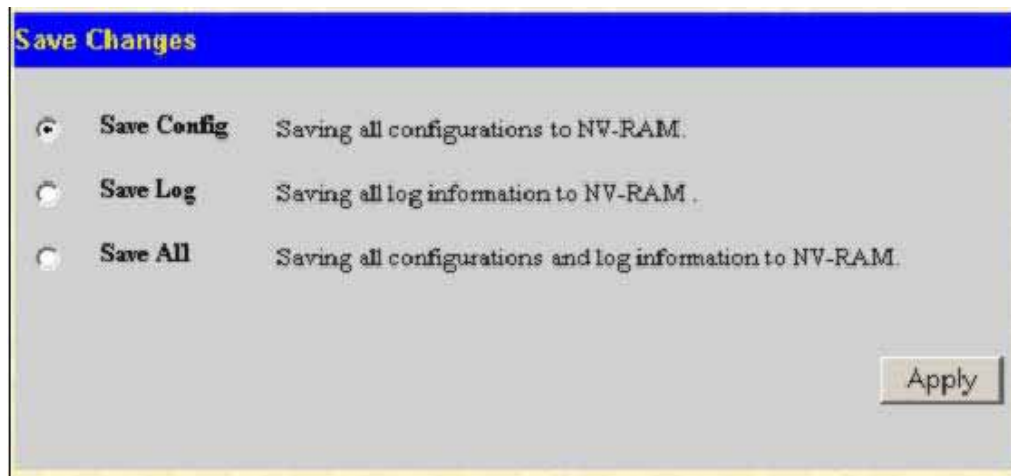



図 11- 31. Save Changes 画面

付録

付録 A

製品の仕様

型番		DES-3010G	DES-3018	DES-3026
標準規格		IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T, IEEE 802.3x Flow Control IEEE 802.3z 1000BASE-LX/SX/LHX/ZX(DES-3010G のみ) IEEE 802.ad Link Aggregration,IEEE 802.1Q VLAN Tagging IEEE 802.1D Spanning Tree(STP compatible) IEEE 802.1X Port Based Network Access Control IEEE 802.1p Case of Service, priority protocol IEEE 802.1w Rapid Spanning Tree		
インタフェース	10BASE/100BASE-TXポート(RJ-45)	8	16	24
	10BASE/100BASE-TX /1000BASE-Tポート(RJ-45)	1	–	–
	オートネゴシエーション	○	○	○
	Auto MDI/MDI-X	○	○	○
	フローコントロール	IEEE 802.3x Flow Control(Full Duplex)、バックプレッシャー(Half Duplex)、ヘッドオブライン(HOL)ブロッキング防止		
	SFP(Mini-GBIC)ポート	1	–	–
	アップリンク用スロット	–	2	
	RS-232C ポート (D-Sub 9 ピンメス)	1		
コネクタ形状	メタルポート	RJ-45 (1000BASE-T)		
	光ポート	LC	–	–
適合ケーブル	10BASE-T	カテゴリ3以上のUTP/STPケーブル(100m以内)		
	100BASE-TX	カテゴリ5以上のUTP/STPケーブル(100m以内)		
	1000BASE-T	エンハンスドカテゴリ5以上のUTP/STPケーブル(100m以内)		
	コンソールポート	RS-232Cストレートケーブル(D-Sub 9ピン)		
仮想スタック	スタック数(最大)	32		
アップリンク（オプション）	1000BASE-T	–	DEM-301T	
	1000BASE-LX	–	DEM-301G	

型番			DES-3010G	DES-3018	DES-3026
	アップリンク数		ー	2	
スイッチ性能	スイッチファブリック		5.6Gbps	7.2Gbps	8.8Gbps
	パケットフォワーディングレート		4.2Mpps	5.4Mpps	6.6Mpps
	パケットバッファ		256KByte		
	MACアドレス数		アドレステーブル：8K、スタティックMACアドレステーブル：256		
	SDRAM		32MByte		
電気的仕様	定格入力電圧		100-240VAC (50/60Hz) ＊ 同梱の電源ケーブルは100V専用です。		
	消費電力（最大）		9.9W	10.5W	11.6W
環境仕様	温度	動作時	0～40℃		
		保管時	-40～70℃		
	湿度	動作時	10～90%（結露なきこと）		
		保管時	5～95%（結露なきこと）		
	寸法		280(W) x 108(D) x 44(H) mm * 19 インチラックマウント 1U 対応	441(W) x 207(D) x 44(H) mm * 19 インチラックマウント 1U 対応	
	質量		1.5kg	2.1kg	
適合規格	EMI 規格		CE/FCC/VCCI/ C-Tick クラス A		

ソフトウェア仕様

機能	内容
L2機能	IGMP スヌーピング: v1、v2、v3 マルチキャストグループ: 256 スタティックマルチキャストグループ:64 スパニングツリー : IEEE 802.1D STP、IEEE 802.1W RSTP STPループバック防御 IEEE 802.3ad リンクアグリゲーション :3グループ、8ポート/グループ ポートミラーリング : 1対1、1対多 BPDUフィルタリング
VLAN	IEEE 802.1Q タグVLAN VLANグループ : スタティックVLAN: 255 Configurable VLAN: 255
QoS	帯域制御 IEEE 802.1p サポート ポートごとに4レベルのキューを装備 ポートベースCoS
セキュリティ	帯域制御: GUI/CLIメッセージリマインド IEEE 802.1Xポートベース/MACベースアクセス制御 トラフィックセグメンテーション、ブロードキャストストームコントロール CPUインタフェースフィルタリング
MIBs	MIB-Ⅱ(RFC 1213) / Bridge MIB (RFC 1493) RMON MIB (RFC 1757,2829) / IF MIB (RFC 2333,2863) IEEE 802.1p MIB (RFC 2674) / Ether-like MIB (RFC 2665) プライベート MIB
マネージメント	D-LinkシングルIPマネージメント v.1.6、Telnetサーバ/ TFTPクライアント WebベースGUI(トラフィックモニタ、MACアドレス検索など) / CLI SNMP : v.1、v.2c、v.3 、RMON v.1 DHCP自動設定、システムログ BootP/DHCPクライアント 、CPUインタフェースフィルタリング トラップ/アラーム/ログレベル設定 show configコマンド、ポートディスクリプション、SNTP SMTPクライアント / 拡張ログ

2 芯 SFP モジュール(オプション)仕様

型番		DEM-310GT	DEM-311GT
標準規格		IEEE 802.3z 1000BASE-LX 、MSA、IEEE 802.3x Flow Control	IEEE 802.3z 1000BASE-SX 、MSA、IEEE 802.3x Flow Control
コネクタ形状		LC	
光波長		1310nm	850nm
送信光レベル/受信光レベル		-9.5～-3dBm/-21～-3dBm	-9.5～-4dBm/-17～-3dBm
受光感度		-21dBm	-7.5dBm
光ファイバケーブルタイプ	2芯シングルモード	9/125μm	—
	2芯マルチモード	—	50/125μm
伝送距離※		10km	550m
動作電圧		3.3V	
入力電流(最大)		300mA	240mA
発熱量		1.78kJ/h	1.54kJ/h
ホットプラグ		○	○
温度	動作時	0～70℃	
	保管時	-40～85℃	
湿度	動作時	10～90%(結露なきこと)	
	保管時	5～90%(結露なきこと)	
寸法		13.4(W) x 56.4(D) x 10.35(H) mm	
質量		16.5g	15.5g
適合規格	EMI規格	FCC クラスB、EN55022 クラスB、VCCI クラスB	

※ 光ファイバケーブルの最長伝送距離は光ファイバ損失分散、光コネクタ、スプライス損失箇所などの総合損失によって異なります。

型番		DEM-312GT2	DEM-314GT	DEM-315GT
標準規格		IEEE 802.3z　1000BASE-SX IEEE 802.3x Flow Control MSA	IEEE 802.3z 1000BASE-LHX IEEE 802.3x Flow Control MSA	IEEE 802.3z 1000BASE-ZX IEEE 802.3x Flow Control MSA
コネクタ形状		LC		
光波長		1310nm	1550nm	
送信光レベル		-9.5～-3dBm	-6～0dBm	0～5dBm
受信光レベル		-23dBm		
受光感度		-21dBm		
光ファイバ ケーブルタイプ	2芯シングルモード	―	9/125μm	
	2芯マルチモード	62.5/125μm	―	―
伝送距離※		2km	50km	80km
動作電圧		3.3V		
入力電流(最大)		300mA		
発熱量		1.78kJ/h	1.90kJ/h	2.37kJ/h
ホットプラグ		○	○	○
温度	動作時	0～70℃		
	保管時	-40～85℃		
湿度	動作時	10～90%(結露なきこと)		
	保管時	5～90%(結露なきこと)		
寸法		13.4(W) x 56.4(D) x 10.35(H) mm		
質量		17.5g	17.8g	
適合規格	EMI規格	FCC クラスB、EN55022 クラスB、VCCI クラスB		

※ 光ファイバケーブルの最長伝送距離は光ファイバ損失分散、光コネクタ、スプライス損失箇所などの総合損失によって異なります。

WDM 対応 1 芯 SFP モジュール(オプション)仕様

型番		DEM-330T	DEM-330R
標準規格		IEEE 802.3z 1000BASE-LX、IEEE 802.3x Flow Control、MSA	
コネクタ形状		LC	
光波長		TX:1550nm、RX:1310nm	TX:1310nm、RX:1550nm
送信光レベル/受信光レベル		-9～-3dBm / -21～-1dBm	
受光感度		-21dBm	
光ファイバケーブルタイプ　1芯シングルモード		9/125μm	
伝送距離※		10km	
動作電圧		3.3V	
入力電流(最大)		300mA	
発熱量		1.78kJ/h	
ホットプラグ		○	○
温度	動作時	0～70℃	
	保管時	-40～85℃	
湿度	動作時	10～90%(結露なきこと)	
	保管時	5～90%(結露なきこと)	
寸法		13.4(W) x 55.5(D) x 11.28(H) mm	
質量		19.8g	
適合規格	EMI規格	FCC/VCCI クラスB、EN55022クラスB	

※ DEM-330T と DEM-330R は対向でご使用ください。

※ 光ファイバケーブルの最長伝送距離は光ファイバ損失分散、光コネクタ、スプライス損失箇所などの総合損失によって異なります。

型番		DEM-331T	DEM-331R
標準規格		IEEE 802.3z 1000BASE-LX、IEEE 802.3x Flow Control、MSA	
コネクタ形状		LC	
光波長		TX:1550nm、RX:1310nm	TX:1310nm、RX:1550nm
送信光レベル/受信光レベル		-3～2dBm / -23～-1dBm	
受光感度		-23dBm	
光ファイバケーブルタイプ　1芯シングルモード		9/125μm	
伝送距離※		40km	
動作電圧		3.3V	
入力電流(最大)		300mA	
発熱量		2.14kJ/h	
ホットプラグ		○	○
温度	動作時	0～70℃	
	保管時	-40～85℃	
湿度	動作時	10～90%(結露なきこと)	
	保管時	5～90%(結露なきこと)	
寸法		13.4(W) x 55.5(D) x 11.28(H) mm	
質量		20.1g	
適合規格	EMI規格	FCC/VCCI クラスB、EN55022クラスB	

※ DEM-331T と DEM-331R は対向でご使用ください。

※ 光ファイバケーブルの最長伝送距離は光ファイバ損失分散、光コネクタ、スプライス損失箇所などの総合損失によって異なります。

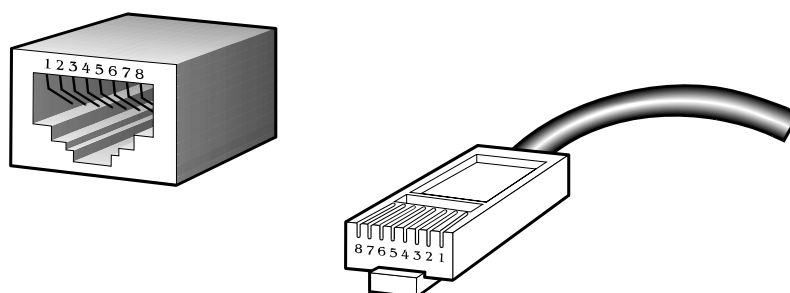
Uplink モジュール(オプション)仕様

型番		DEM-301T	DEM-301G
標準規格		IEEE 802.3ab 1000BASE-T	IEEE 802.3z 1000BASE-LX
インタフェース		1000BASE-T x 1ポート	SFP x 1ポート
コネクタ形状		RJ-45	LC
寸法		150(W) x 57(D) x 28(H) mm	
適合規格	EMI規格	FCC/VCCI クラスA、CE、C-Tick	

付録 B

ケーブルとコネクタ

スイッチを別のスイッチ、ブリッジまたはハブに接続する場合、ノーマルケーブルが必要です。ケーブルピンアサインに合うことを再確認してください。

以下の図と表は標準のRJ-45 プラグ/コネクタとピンアサインです。

付録 1- 1. 標準の RJ-45 プラグとコネクタ

RJ-45 ピンアサイン		
コンタクト	MDI-X 信号	MDI-II信号
1	BI-DB+	BI-DA+
2	BI-DB-	BI-DA-
3	BI-DA+	BI-DB+
4	BI-DD+	BI-DC+
5	BI-DD-	BI-DC-
6	BI-DA-	BI-DB-
7	BI-DC+	BI-DD+
8	BI-DC-	BI-DD+

付録 1- 2. 標準 RJ-45 ピンアサイン

付録C

ケーブル長

以下の表は各規格に対応するケーブル長(最大)です。

準拠規格	メディアタイプ	最大距離
Mini-GBIC	1000BASE-LX，シングルモード光ファイバモジュール 1000BASE-SX，マルチモード光ファイバモジュール 1000BASE-LHX，シングルモード光ファイバモジュール 1000BASE-ZX，シングルモード光ファイバモジュール	10km 550m 40km 80km
1000BASE-T	エンハンスドカテゴリ5 UTPケーブル カテゴリ5 UTPケーブル(1000 Mbps)	100m
100BASE-TX	カテゴリ5 UTPケーブル（100 Mbps)	100m
10BASE-T	カテゴリ3 UTPケーブル（10 Mbps)	100m

用語解説

1000BASE-LX: 最大伝送速度 1Gbps の Gigabit Ethernet の規格のひとつ。長い光波長で長距離伝送用に使用されます。伝送距離(最大)はシングルモード光ファイバを使用した場合で 10km。

1000BASE-SX: 最大伝送速度 1Gbps の Gigabit Ethernet の規格のひとつ。短い光波長でマルチモード光ファイバを使用した場合伝送距離(最大)は 550km。

100BASE-FX:光ファイバを使用する最大伝送速度 100Mbps の Fast Ethernet の規格のひとつ。

100BASE-TX:カテゴリ 5 以上の UTP ケーブルを使用する最大伝送速度 100Mbps の Fast Ethernet の規格のひとつ。

10BASE-T: IEEE 802.3 準拠でカテゴリ 3 以上の UTP ケーブルを使用する最大伝送速度 10Mbps の Ethernet の規格のひとつ。

エージング: タイムアウトし、無効のスイッチのダイナミックデータベースを自動的に消去します。

ATM: 非同期転送モード。セルと呼ばれる固定長のセル(パケット)ベースで転送するプロトコル。ATM は音声、データおよびビデオ信号を含むユーザトラフィックの完全な列を転送するために開発されたものです。

オートネゴシエーション:スピード、デュプレックスおよびフローコントロールを自動的に認識する機能。オートネゴシエーションをサポートする端末と接続すると、リンクは自動的に最適なリンク条件に設定されます。

バックボーンポート: デバイスのアドレスを学習せず不明なアドレスを持つすべてのフレームを受信するポート。バックボーンポートは通常ご使用のネットワークのバックボーンにスイッチを接続するために使用されるポートです。バックボーンポートは以前はダウンリンクポートとして知られていました。

バックボーン: ネットワークセグメント間でトラフィックが転送される場合に優先パスとして使用されるネットワークの一部分。

帯域: 1 秒あたりのビット数で計算される 1 チャンネルが転送できる情報量。イーサネットの帯域は 10Mbps、ファーストイーサネットは 100Mbps。

ボーレート: ラインのスイッチングスピード。ネットワークセグメント間のラインスピードとして知られています。

BOOTP: BOOTP プロトコルはデバイスが起動するたびに IP アドレスを MAC アドレスに自動マッピングします。さらにデバイスにサブネットマスク、デフォルトゲートウェイを割り当てます。

ブリッジ: たとえ高いレベルのプロトコルが関連してもローカルまたはリモートネットワークを相互接続するデバイス。ブリッジはネットワーク管理を中央に集めて 1 個の論理ネットワークを形成します。

ブロードキャスト: ネットワーク上のすべての終点デバイスに送信されるメッセージ。

ブロードキャストストーム:が主として可能なネットワーク帯域を奪い、ネットワークエラーを引き起こす Multiple simultaneous ブロードキャスト。

コンソールポート: 端末またはモデムコネクタと接続可能なスイッチ上のポート。コンピュータ内でパラレル配列のデータをデータ転送リンクで使用されるシリアル形式に変換します。このポートはほとんどの場合ローカル管理のために使用されます。

CSMA/CD:イーサネットと IEEE 802.3 標準によって使用されるチャンネルアクセス方法で検索したデータチャンネルが一定期間後クリアされた後にだけデバイスに転送します。2 つのデバイスが同時に転送する場合、コリジョンが発生し、コリジョンを発生したデバイスは任意の時間再転送を遅らせます。

データセンタースイッチング: スイッチがサーバファームへの高パフォーマンスアクセス、高速バックボーン接続、およびネットワーク管理とセキュリティのためのコントロールポイントを提供するコーポレートネットワーク内のアグリゲーションポイント

イーサネット: Xerox、Intel および DEC が共同で開発した LAN 仕様。イーサネットネットワークは CSMA/CD を使用して 10Mbps で処理を行います。

ファーストイーサネット: Ethernet/CD ネットワークアクセス方法をベースにした 100Mbps 技術。

フローコントロール: (IEEE 802.3z) 端末に接続した転送ポートへのパケットを抑止します。受信バッファがあふれそうになった場合にパケットロスを防ぎます。

フォワーディング:中間のネットワークデバイスによりパケットを到達点に向けて送信するプロセス。

フルデュプレックス: 同時にパケットの送受信を可能とし、スループットを 2 倍にするシステム。

ハーフデュプレックス: パケットの送受信を行うが、同時には行えないシステム。

IP アドレス: Internet Protocol アドレス。TCP/IPを使用するネットワークに付属するデバイスの固有な識別子。IPv4 アドレスは 8 ビットずつピリオドで区切られ、ネットワークセクション、サブネットセクション、ホストセクションで構成されます。

IPX - **Internetwork Packet Exchange**:ネットワーク通信で使用するプロトコル。

LAN – ローカルエリアネットワーク: 通常フロアもしくはビルのような規模の小さいエリアで PC、プリンタ、サーバのようなコンピュータリソースを接続するネットワーク。高速で低エラー率が特長です。

レイテンシ: デバイスがパケットを受信する時間とパケットが到達点ポートに転送される時間の遅延。

ラインスピード: ボーレートを参照。

メインポート: 通常の操作条件でデータトラフィックを送信する Resilient リンク内のポート。

MDI - Medium Dependent Interface: 1 つのデバイスの送信装置が別のデバイスの受信装置に接続するイーサネットポート接続。

MDI-X - **Medium Dependent Interface Cross-over**: 接続送受信のラインが交差しているイーサネットポート接続。

MIB - Management Information Base: デバイスの管理特性とパラメータを保持します。MIB は SNMP で使用され、管理システムの属性を持っています。スイッチは自身の内部 MIB を持っています。

マルチキャスト: シングルパケットはネットワークアドレスの特定のサブセットにコピーします。これらのアドレスはパケットの到達点アドレス内に記述されます。

プロトコル: ネットワーク上のデバイス間通信のルール。ルールは形式、タイミング、配列およびエラー制御を定義しています。

Resilient link: 他のポートがエラーになった場合に一方のポートがデータ転送を引き継ぐように設定された 1 対のポート。

RJ-45: 10BASE-T や 100BASE-TX などで使用する標準 8 線コネクタ

RMON: リモート監視。SNMP MIB II のサブセットはアドレッシングによって異なる最大 10 個のグループまでのモニタリングや管理を可能にします。

RPS – リダンダント電源システム: スイッチに接続されて、バックアップ電源を供給するデバイス。

サーバファーム: 大量のユーザにサービスを提供する中央に位置するサーバグループ。

SLIP - **Serial Line Internet Protocol:** IP がシリアルライン接続を経由して動作することが可能なプロトコル。

SNMP - Simple Network Management Protocol:当初は TCP/IP インターネットを管理するために開発されたプロトコル。SNMP は現在広範囲のコンピュータとネットワークの装置で実行され、多くのネットワークおよび端末操作の状況を管理するために使用されます。

スパニングツリープロトコル (STP): ネットワーク上のフォールトトレランスを提供するブリッジベースのシステム。STP はネットワークトラフィックに対してパラレルパスを実行し、メインのパスにエラーが発生してもメインのパスが操作できる場合はリダンダントパスを無効にすることを保証します。

スタック: 1 個の論理的なデバイスの形をとするために統合されたネットワークデバイスのグループ。

スタンバイポート: リンクしているメインポートにエラーが発生すると、Resilient リンク内のスタンバイポートはデータ転送を受け継ぎます。

スイッチ: パケットの終点アドレスを元にパケットのフィルタ、フォワードするデバイス。スイッチは各スイッチポートで関連するアドレスを学習し、この情報を元に表を作成してスイッチの決定に使用します。

TCP/IP: Telnet 端末エミュレーション、FTP ファイル転送などコンピュータ装置の広い範囲で通信サービスを提供する通信プロトコルです。

telnet: 仮想端末サービスを提供する TCP/IP アプリケーションプロトコルで、ユーザが別のコンピュータシステムにログインし、ユーザが直接ホストに接続しているようにホストにアクセスすることができます。

TFTP - Trivial File Transfer Protocol: スイッチのローカルの管理能力を使用してリモートデバイスからファイルを転送する(ソフトウェアアップグレードなど)ことができます。

UDP - User Datagram Protocol:インターネットの標準プロトコルで、あるデバイスのアプリケーションプログラムがデータを別のデバイス上のアプリケーションプログラムに送信することができます。

VLAN - Virtual LAN: 物理的に接続した LAN のように通信する位置やトポロジーが独立しているデバイスのグループ。

VLT - Virtual LAN Trunk: 各スイッチ上のすべての VLAN トラフィックを転送するスイッチ間のリンク。

VT100: ASCIIコードを使用するターミナルタイプ。 VT100 画面はテキストベースの表示をします。

International Offices

U.S.A
17595 Mt. Herrmann Street
Fountain Valley, CA. 92708
TEL: 714-885-6000
Fax 866-743-4905
URL: www.dlink.com
Canada
2180 Winston Park Drive
Oakville, Ontario, L6H 5W1
Canada
TEL: 1-905-8295033
FAX: 1-905-8295223
URL: www.dlink.ca
Europe (U. K.)
4th Floor, Merit House
Edgware Road, Colindale
London NW9 5AB
U.K.
TEL: 44-20-8731-5555
FAX: 44-20-8731-5511
URL: www.dlink.co.uk
Germany
Schwalbacher Strasse 74
D-65760 Eschborn
Germany
TEL: 49-6196-77990
FAX: 49-6196-7799300
URL: www.dlink.de
France
Le Florilege #.2, Allee de la Fresnerie
78330 Fontenay le Fleury
France
TEL: 33-1-30238688
FAX: 33-1-30238689
URL: www.dlink-france.fr
Netherlands
Weena 290
3012 NJ Rotterdam
Netherlands
Tel: +31-10-282-1445
Fax: +31-10-282-1331
URL: www.dlink-benelux.com
Belgium
Rue des Colonies 11
B-1000 Brussels
Belgium
Tel: +32(0)2 517 7111
Fax: +32(0)2 517 6500
URL: www.dlink-benelux.com
Italy
Via Nino Bonnet n. 6/b
20154 – Milano,
Italy
TEL: 39-02-2900-0676
FAX: 39-02-2900-1723
URL: www.dlink.it
Sweden
P.O. Box 15036, S-167 15 Bromma
Sweden
TEL: 46-(0)8564-61900
FAX: 46-(0)8564-61901
URL: www.dlink.se

Denmark
Naverland 2, DK-2600
Glostrup, Copenhagen,
TEL: 45-43-969040
FAX: 45-43-424347
URL:www.dlink.dk
Norway
Karihaugveien 89
1086 Oslo
Norway
TEL: 47-23-897189
FAX: 47-22-309085
URL: www.dlink.no
Iberia
C/Sabino De Arana,
56 Bajos
08028 Barcelona
TEL: 34 93 4090770
FAX: 34 93 4910795
URL: www.dlinkiberia.es
Singapore
1 International Business Park
#03-12 The Synergy
Singapore 609917
TEL: 65-6774-6233
FAX: 65-6774-6322
URL: www.dlink-intl.com
Australia
1 Giffnock Avenue,
North Ryde, NSW 2113
Australia
TEL: 61-2-8899-1800
FAX: 61-2-8899-1868
URL: www.dlink.com.au
India
D-Link House, Kurla Bandra Complex Road,
Off CST Road, Santacruz (East), Mumbai - 400098.
India
TEL: 91-022-26526696/56902210
FAX: 91-022-26528914
URL: www.dlink.co.in
Middle East (Dubai)
P.O.Box: 500376
Office No.:103, Building:3
Dubai Internet City
Dubai, United Arab Emirates
Tel:+971-4-3916480
Fax:+971-4-3908881
URL: www.dlink-me.com
Turkey
Maslak Ayazaga Yolu
No: 2 Kat :5
Ayazaga-Istanbul
TURKEY
TEL: 0090 212 289 56 59
FAX: 0090 212 289 76 06
URL: www.dlink.com.tr
Egypt
19 El-Shahed Helmy, El Masri
Al-Maza, Heliopolis
Cairo,Egypt.
TEL:+202 414 4295
FAX:+202 415 6704
URL: www.dlink-me.com

Israel
11 Hamanofim Street
Ackerstein Towers, Regus Business Center
P.O.B 2148, Hertzelia-Pituach 46120.
Israel
TEL: +972-9-9715700
FAX: +972-9-9715601
URL: www.dlink.co.il
Latin America
Isidora Goyeechea 2934 of 702,
Las Condes
Santiago – Chile S.A.
TEL: 56-2-232-3185
FAX: 56-2-232-0923
URL: www.dlink.cl
Brasil
Av das Nacoes Unidas,
11857 - 14 - andar - cj 141/142
Brooklin Novo
Sao Paulo - SP - Brazil
CEP 04578-000
TEL: +55 11 55039320
FAX: +55 11 55039322
URL: www.dlinkbrasil.com.br
South Africa
Einstein Park II
Block B
102-106 Witch-Hazel Avenue
Highveld Technopark
Centurion
Gauteng
Republic of South Africa
TEL: 27-12-665-2165
FAX: 27-12-665-2186
URL: www..d-link.co.za
Russia
Grafsky per., 14, floor 6
Moscow
129626 Russia
TEL: 7-095-744-0099
FAX: 7-095-744-0099 #350
URL: www.dlink.ru
China
No.202,C1 Building, Huitong Office Park,
No.71, Jianguo Road, Chaoyang District, Beijing,
100025, China.
TEL +86-10-58635800
FAX: +86-10-58635799
URL: www.dlink.com.cn
Taiwan
2F, No. 119, Pao-Chung Rd.
Hsin-Tien, Taipei
Taiwan
TEL: 886-2-2910-2626
FAX: 886-2-2910-1515
URL: www.dlinktw.com.tw
Headquarters
2F, No. 233-2, Pao-Chiao Rd.
Hsin-Tien, Taipei
Taiwan
TEL: 886-2-2916-1600
FAX: 886-2-2914-6299
URL:www.dlink.com

DLJ-06Q2-ESMA006/A.01